Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Využití biometrických prvků pro identifikaci osob v oblasti elektromobility.

Application of Biometric Components for Personal Identification in Electromobility Area

Ostrava 2015 Karolína Janošová

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Zadání bakalářské práce

Student: **Karolína Janošová**

Studijní program: B2649 Elektrotechnika

Studijní obor: 3901R039 Biomedicínský technik

Téma: Využití biometrických prvků pro identifikaci osob v oblasti elektromobility
Application of Biometric Components for Personal Identification in Electromobility Area

Zásady pro vypracování:

1. Seznámení se s problematikou biometrické identifikace osob.
2. Seznámení se s problematikou elektromobility a její infrastruktury, zejména pak se současnými trendy v oblasti identifikace řidiče nebo obsluhy elektromobilu.
3. Seznámení se s problematikou bezpečnosti elektrických zařízení a z toho vyplývajících omezení.
4. Návrh řešení biometrické identifikace uživatele.
5. Realizace funkčního modelu zařízení pro biometrickou identifikaci uživatele.
6. Zhodnocení dosažených výsledků práce.

Seznam doporučené odborné literatury:

[1] GREGORY, Peter H. a Michael A. SIMON. *Biometrics for dummies*. Hoboken : Wiley Publishing Inc., 2008. xvi, 292 p. ISBN 978-0-470-29288-4.
[2] JAIN, A.K., R. BOLLE a S. PANKANTI, eds. *Biometrics: personal identification in networked society*. Boston: Kluwer, c1999, x, 411 p. ISBN 978-0387-28539-9.
[3] JAIN, Anil K. *Introduction to biometrics*. New York: Springer, c2011, xvi, 311 s. ISBN 978-0-387-77325-4.
[4] MODI, Shimon K. *Biometrics in identity management: concepts to applications*. Boston: Artech House, c2011, xiv, 263 p. Artech House information security and privacy series. ISBN 978-1-60807-017-6.
[5] MADDALA, S., J.S. BARTUNEK a M. NILSSON. *Biometric Fingerprint Recognition Fingerprint Recognition using C-language MEX-Files*. neue Ausg. Saarbrücken: VDM Verlag Dr. Müller, 2010. ISBN 978-3639318074.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Pavlína Nádzíková**

Datum zadání: 01.09.2014

Datum odevzdání: 07.05.2015

doc. Ing. Jiří Koziorek, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Čestné prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně. Veškeré použité podklady, ze kterých jsem čerpala informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V Ostravě dne 7. 5. 2015

Karolína Janošová

Karolína Janošová

Poděkování

Děkuji Ing. Pavlíně Núdzikové a za odborné vedení práce, věcné připomínky, dobré rady. Ing. Davidu Valovi za odborné vedení, vstřícnost při konzultacích a vypracovávání bakalářské práce. Poděkování patří také rodině, za pochopení a podporu při studiu.

Abstrakt

Bakalářská práce řeší problematiku biometrické identifikace a verifikace osob. Zaměřuje se na rozpoznávání pomocí otisku prstu. Rozpoznávání je řešeno v oblasti elektromobility. Cílem práce je najít vhodný senzor otisku prstu pro vytvoření hardwaru. Pro tento senzor dále navrhnout a vytvořit program vhodný pro identifikaci a verifikaci osob.

Po průzkumu trhu byl nalezen vhodný senzor. Pomoci převodníku je spojen s počítačem. Následuje vývoj programu pro rozpoznávání a identifikaci osob. Poté bude doplněn o databázi údajů uživatelů.

Klíčová slova

identifikace osob, využití biometrických údajů, biometrické údaje, biometrie, elektromobilita, otisky prstů, senzor otisku prstu

Abstract

This thesis solves the issue of biometric identification and verification of people. The thesis focuses on Fingerprint recognition. The recognition is solved in Electromobility Area. The goal of this thesis is to discover a suitable fingerprint sensor for using in the hardware part. For fingerprint sensor will be designed and created an appropriate program for identification and verification of persons.

We was found the suitable fingerprint sensor, after the market research. Sensor is connected to the computer with other component. This part of thesis is followed by the development of the program for verification and identification. Then it will be complemented by a database of data users.

Keywords

identification of persons, the use of biometrics, biometric data, biometrics, electromobility, fingerprints, fingerprint sensor

Seznam použitých zkratek a symbolů

apod. - a podobně

1 bit (b) - základní, nejmenší jednotkou datového toku; udává např. barevnou hloubku obrazu (uvádí se počet bitů, které zabere v paměti číslo, definující jas jednoho pixelu)

1 byte (B)- jednotka digitálních informací v počítači a telekomunikacích; skládá se z osmi bitů

1 dpi= počet bodů na palec, hustota obrazové informace

1 megahertz (MHz)- jednotka frekvence

C#- vysokoúrovňový objektově orientovaný programovací jazyk

CPIT- Vědecko-výzkumné laboratoře Vysoké školy báňské

FAR (%)- míra chybného přijetí

FRR (%)- míra chybného odmítnutí

např. - například

RS232- sériové komunikační rozhraní

tzv. - takzvaný

UART- univerzální asynchronní přijímač / vysílač, kus počítačového hardwaru, který překládá data mezi paralelními a sériovými forem.

USB- univerzální sériová sběrnice, moderní způsob připojení periferií k počítači

Obsah

Úvod

Tématem bakalářské práce je využití biometrických prvků pro identifikaci osob v oblasti elektromobility. Základním prvkem práce je tudíž využití biometrie. Biometrie je věda, která využívá charakteristické měřitelné biologické struktury lidského těla k rozpoznávání osob. Toto rozpoznávání je možné například podle hlasu, otisku prstu, oční duhovky, geometrie ruky či kombinací jiných měřitelných prvků. Tato věda vychází z tvrzení, že tyto měřitelné struktury by měly být pro každou osobu jedinečné a unikátní. Díky tomu je každý člověk svým vlastním jediným originálem.

Biometrie se využívá v mnoha oblastech života, především v kriminalistice pro identifikaci pachatelů trestných činů. Dále také v odvětví průmyslu, pro různorodé bezpečnostní a přístupové systémy. Zde je využíván zejména otisk prstu. Prst ruky má totiž charakteristické, takzvané papilární linie. Díky jejich specifické stavbě a struktuře lze rozlišit každého jedince. Měříme vzdálenost papilárních linií, jejich zakřivení a počet v určité oblasti prstu.

Biometrie je využívána také v oblasti elektromobility a vozidlových systémů. Využívá se pro systémy aktivní bezpečnosti, autorizace řidiče a posádky vozidla, komfortní systémy, a systémy pro sledování příznaků únavy řidiče apod. Různé bezpečnostní systémy jsou dnes běžně užívány pro detekci osob při sezení na sedadlech auta, v souvislosti s aktivací airbagů či aktivaci kontrolky zapnutí bezpečnostních pásů.

Pro získání otisků prstů se používají speciální snímače či senzory. Tyto senzory jsou realizovány pomocí mnoha metod snímání, např. optická, kapacitní, tlaková či teplotní apod. Senzory lze dělit také podle typů snímání. Řadíme zde daktyloskopické karty s tzv. rolováním otisků prstů, dále statické a dynamické snímání.

Pro tuto práci proběhl průzkum trhu týkající se biometrické techniky. Výběr čidla proběhl dle specifických parametrů. Mezi tyto parametry řadíme míru chybného přijetí, míru chybného odmítnutí, komunikační rozhraní, typ snímače a metodu snímání. Pro tuto práci jsme vybrali senzor, který funguje na principu statického snímání s užitím optické metody snímání. Tento senzor je kontaktní.

Čidlo bylo následně zprovozněno a probíhá testování funkčnosti. Další část je sestavení programu pro propojení senzoru s počítačem a program pro identifikace a verifikaci osob.

Program je vytvářen pomocí programovacího jazyka C#. Hlavní část programu tvoří rekognice a identifikace osob. Program je tvořen ve vývojovém prostředí Microsoft Visual Studio 2013. K programu je připojena databáze. Problematika databáze je řešena díky aplikaci phpMyAdmin.

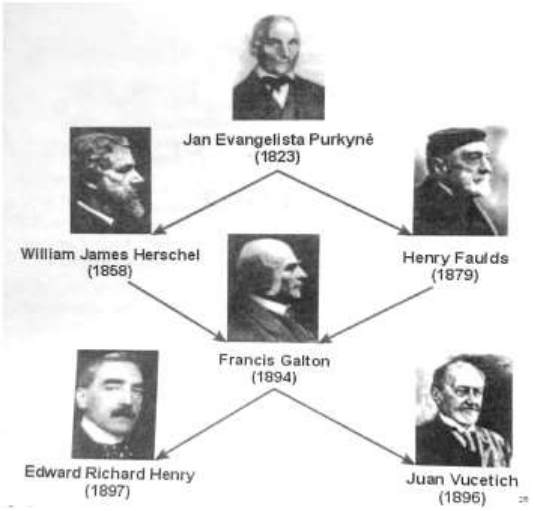
Aplikace phpMyAdmin je nástroj pro správu MySQL databáze. MySQL databáze slouží k ukládání dat uživatelů. Správa databáze probíhá v prostředí HeidiSQL. Prostředí je určené pro práci s MySql databázemi. Umožňuje práci s tabulkami a jejich obsahy.

1. Biometrie

Biometrie je věda využívající charakteristických biologických struktur lidského těla k rozpoznávání osob. Název biometrie vznikl ze spojení řeckých slov „metron“ tedy měření a „bios“ neboli život. Jedná se o měření fyziologických vlastností lidského těla. Teorie biometrie vychází z přesvědčení, že dané biometrické znaky jsou nezaměnitelné. Pro každého člověka by tudíž měly být unikátní.

1.1. Historie biometrie

Biometrické charakteristiky a jejich užití existují odpradávna. Rozeznat osoby jsme schopni podle hlasu nebo obličeje. Archeologicky doložené důkazy o prvním využívání biometrie řadíme do období datovaných před naším letopočtem. Nálezy z Číny jsou datovány do 14. století před naším letopočtem. Kresby, objevené na skalních stěnách, jsou doprovázeny útvary připomínající otisky prstů. Tyto stopy mohly dokazovat autorství kreseb. Jisté stopy využívání jakýchkoliv biometrických údajů byly nalezeny na území Asyrského státu, datované do 9. století. Další nálezy pocházejí z Egypta, Římské říše či Řecka. Ve většině doložených zdrojů se jedná především o využití otisků bříšek prstů horní končetiny. Nejstarší nálezy otisků lidské ruky jsou z oblasti státu Indiana v Americe. Tyto „petroglyfy“ jsou staré pravděpodobně i několik tisíciletí. Poprvé se otisky prstů používali k identifikaci osob v Babylonu za vlády královny Hanimurabi v 18. století před naším letopočtem. První dokument o této metodě pochází od čínského autora Kio Kung-yen. Čína byla v tomto odvětví velmi vyspělá. Využívali tuto metodu při obchodních, úředních či kriminalistických záležitostech.



Obrázek 1: Schématické zobrazení významných daktyloskopů [2]

Věda**,** která se zabývá kožními papilárními liniemi na prstech, dlaních ruky a ploskách nohou se nazývá daktyloskopie. První vědecké spisy řešící tuto problematiku se objevují roku 1686. Sepsané

byly Marcellem Malpighim, profesorem anatomie. Významnou osobností v této oblasti je Jan Evangelista Purkyně. Zkoumáním kožních struktur významně přispěl do dějin kriminalistiky a daktyloskopie. Roku 1858 William James Herschel používal otisky prstů k identifikaci zaměstnanců z důvodu negramotnosti dělníků. Hlavními osobnostmi moderní historie biometrie jsou Alphonse Bertillon a Francis Galton. Alphonse Bertillon zavedl postup zvaný Bertillionáž. Jednalo se o měření fyzických rysů těla. Využívala se k identifikaci pachatelů v kriminalistice. Metoda, využívána po celém světě, byla později ukončena. Bylo zjištěno, že dvě osoby mohou mít stejné parametry, tudíž je možná záměna. Již zmíněný vědec, Francis Galton**,** studoval fyzické vlastnosti a jejich dědičnost. Roku 1892 publikoval spis „Fingerprints“, který napomohl zavedení daktyloskopie do praxe. Francis Galton spočítal, že existuje 64 miliard variant otisků prstů. Roku 1900 byla daktyloskopie zařazena do policejní praxe. Tomuto kroku také významně přispěli Edward Richard Henry či Juan Vucetich. Jde především o význam v oddělení identifikace a verifikace osob.

1.2. Charakteristika biometrie

Charakteristika biometrie je dělena do dvou částí. Patří zde fyziologická a behaviorální charakteristika. V případě fyziologické charakteristiky jde o měřitelné údaje. Tyto charakteristiky jsou stálé neboli statické. Zahrnují: otisk prstu, oční duhovku, dlaň a její geometrie, topografie tváře, vůně a zápach, genetický kód DNA, tvary a rozměry těla- obvod hlavy, délka končetin, výška v sedu, apod. Oproti tomu behaviorální charakteristika se zabývá vědomostmi a dovednostmi člověka. Tyto charakteristiky mohou být proměnné v čase. Jedná se o psaní rukou, podpis, psaní na klávesnici, hlas. Pro využití biometrických znaků v izometrických systémech je převážně využíváno fyziologických charakteristik.

1.3. Identita

Slovo identita má původ v latinském jazyce. Z pojmu „idem“, přeloženo „stejný“, vzniklo „identitas“. Nyní používáno v souvislosti s totožností, při porovnávání pojmů, subjektů, objektů, apod.

Identita osoby je jasná charakteristika každého lidského subjektu. Lze dělit na fyzickou identitu a identitu elektronickou. Fyzická identita je dána fyziologickou a behaviorální charakteristikou. Neexistuje jedinec, který má tuto charakteristiku souhlasnou. V případě elektronické identity toto tvrzení není platné. Ve světě elektroniky a internetových sítí je možno stvořit nekonečné množství identit.

1.4. Biometrická identifikace a verifikace

Tyto dva pojmy mají úzký vztah s identitou osoby. Jsou využívány v oblasti biometrických systémů.

1.4.1. Biometrická identifikace

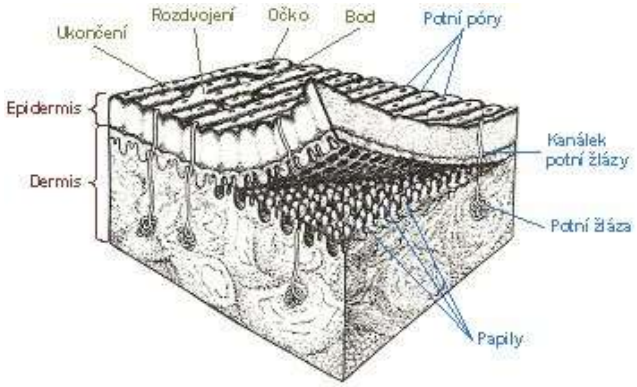
Identifikace je proces porovnávání jeden ku mnoha, tzv. rekognice. Porovnává se vstupní vzorek se všemi vzorky v databázi. Jde tedy o zjištění, zda se jedna snímaná šablona shoduje s jednou z mnoha referenčních šablon obsažených v databázi. Je to „vyhodnocení identity objektu ve vztahu k dalším objektům“. Rozhodovací proces zjišťování identity je poměrně náročný. U rozsáhlejších databází musí být brán v úvahu především čas, za který lze nalézt výsledky. Cílem identifikace jsou dva stavy: „nalezení konkrétní identity“ nebo „nenalezení konkrétní identity“. [1] [2]

1.4.2. Biometrická verifikace

V případě verifikace jde o porovnání jeden ku jedné, neboli autentizace. Porovnáván je jediný vkládaný vzorek s jedinou referenční šablonou. Tato šablona jsou již vložené biometrické znaky porovnávané osoby. Verifikace je proces využití jedinečných, měřitelných, fyzikálních nebo fyziologických znaků (tzv. markantů) nebo projevů člověka k ověření jeho identity. Musí být nalezena dostatečná shodnost vzorků. Podobně jako v případě identifikace je zde důležitý rozhodovací proces. Je vyhodnocen identifikační závěr. Dle měřitelných znaků, vypracovaných metod a specifických algoritmů zde dojde k rozhodnutí, zda porovnávané šablony mají dostatečnou shodu. Tu pak systém vyhodnotí jako přijetí či odmítnutí vkládaného znaku (autorizace objektu). [1] [2]

2. Otisk prstu

Je to vzor tvořený seskupením specifických linií, tzv. papilárních linií. Jsou to charakteristické vyvýšeniny pohybující se v rozmezí 0,1-0,4mm. Co se týče šíře, je uváděno 0,2-0,5mm. Genetická informace těchto struktur je uložena hluboko v pokožce. Proto dochází při obnově pokožky pravidelně i k obnově těchto vzorů. Díky této skutečnosti je zřejmé, že otisky prstů nelze lehce poškodit. Lze tak učinit v případě použití velice násilných metod. Tato unikátní struktura odolá mechanickému vlivu i poleptání. Po procesu regenerace dochází k obnovení struktury otisku, pokud nedošlo k poškození zárodečné vrstvy struktury kůže. [1][3]

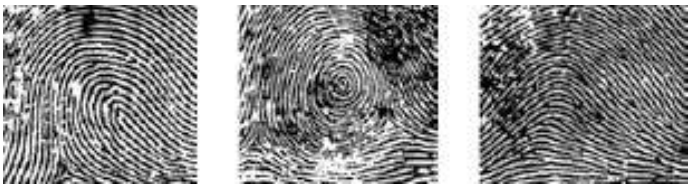


Obrázek 2: Řez kůží a zobrazení průběhu papilárních linií [1]

2.1. Rozlišení papilárních linií a klasifikace

Ve stavbě papilárních linií otisku prstu jsou rozlišovány určité struktury, díky kterým je možno od sebe odlišit jednotlivé otisky prstů. Existují otisky prstů, které nejsou vhodné pro automatické rozpoznávání. Jde zde o osoby trpící různými chorobami. Zde řadíme onemocnění kůže související s poruchami na povrchu pokožky bříška prstu.

Papilární linie otisku prstu vytvářejí specifické vzory. Těmto vzorům se říká tzv. třídy otisků prstů. Existují tyto třídy: oblouk, klenutý oblouk (strmý oblouk), vír (spirála, závit), levá smyčka, pravá smyčka. [1][2][3]



Obrázek 3: Třídy otisků prstů [18]

Tento klasifikační systém vznikl zejména pro snazší prohledávání obsáhlejších databází. Otisky lze totiž zařadit do tříd, a vyhledávání může probíhat pouze v dané třídě.

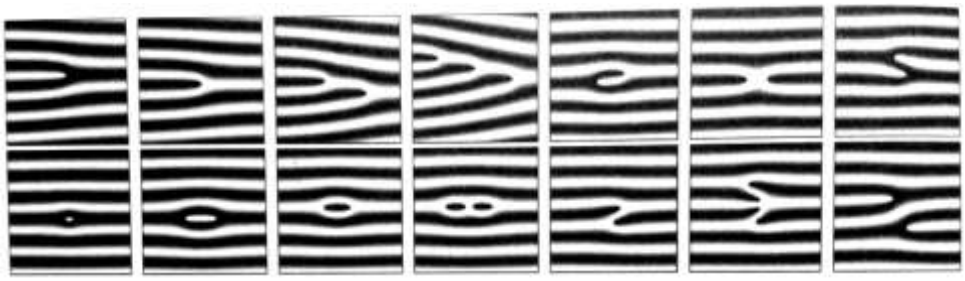
Další pojmy řazené do systému klasifikace se nazývají delta, jádro a typové linie. Delta je oblast, kde jsou papilární linie orientované do tří směrů. Delty bývají většinou na okraji**,** mohou se vyskytovat v otisku i dvakrát. Jádro otisku je střed, jedná se o nejspodnější vyklenutí v průběhu papilárních linií. Jde však o pomyslný střed**,** není to skutečný střed obrázku. Typové linie lemují prostor mezi nejsvrchnější papilární linií patřící ke středu a nejspodnější linií patřící k deltě.

Počet papilárních linií, mezi dvěma danými body, slouží jako metrický údaj doplňující klasifikační systém. Počet papilárních linií se měří v horizontálním i vertikálním směru. Směrem k jádru se počet linií zvětšuje, stejně jako u soustředných letokruhů. Linie se počítají většinou v oblasti mezi jádrem a deltou. Na obrázku vlevo: třídy do sekcí pro možnost měření počtu papilárních linií; vpravo: důležité rysy otisku prstu. [1]

Obrázek 4: Ukázka počtu papilárních linií; Důležité rysy otisku prstu [1]

2.1.1. Identifikace markantů

Vlastní identifikace je prováděna pomocí tzv. markantů (daktyloskopické markanty). Markanty jsou individuální znaky umožňující unikátní struktury papilárních linií. Díky velkému množství markantů v jednotlivých šablonách je snadnější jednotlivé obrazy od sebe rozlišit. Umístění těchto specifických znaků se liší geometrickým tvarem, četností výskytu. Taktéž konkrétní útvary mohou vykazovat rozdíly. Mezi základní markanty řadíme: ukončení, jednoduchá vidlička (rozdvojení), dvojitá vidlička, trojitá vidlička, hák, křížení, boční kontakt (na obrázku horní řada, popis zleva). Spodní řada: bod, interval, jednoduchá smyčka, dvojitá smyčka, jednoduchý most, dvojitý most, průsečná linie. [1][2]



Obrázek 5: Základní typy markantů [1]

3. Snímání otisku prstu

Snímání otisku prstů je dnes aplikováno do nejrůznějších technických zařízení. Je realizováno pomocí senzorů. Senzory jsou různorodá zařízení fungující na rozlišných fyzikálních principech. Dle způsobu kontaktu senzoru s vyšetřovanou tkání, rozdělujeme senzory na kontaktní a bezkontaktní.

Mezi kontaktní senzory řadíme tyto metody: optické, elektronické, opto-elektronické, kapacitní, tlakové a teplotní. Tyto senzory využívají nerovnoměrnosti povrchu pokožky. Z ní vystupují papilární linie. Ty tvoří hřebenovité výstupky vystupující více na povrch. Oproti nim zde jsou také prostorové prohlubně neboli brázdy. Význam má zde také plastičnost povrchu a fyzikální vlastnosti kůže.

Bezkontaktní senzory využívají zejména optické a ultrazvukové metody.

3.1. Metody snímání

Otisky prstů se dají snímat různými metodami. Dnes jsou v biometrických systémech pro snímání obrazu používány snímače otisků prstů. Snímací senzory využívají statického a dynamického snímání nebo snímání šablonováním. Existuje také výjimka v podobě daktyloskopické karty.

3.1.1. Snímání užitím daktyloskopických karet

Jedná se o papírovou kartu, na níž je prst otisknut tzv. rolováním (tj. přiložení prstu a sejmutí otisku téměř od jednoho okraje nehtu až po druhý okraj). Prst je rolován, aby vznikl co nejlepší obraz. Tento obraz je pak skenován do počítače pomocí skeneru. [2]

3.1.2. Statické snímání

Tato metoda je nejčastěji používaná. Jedná se o pouhé přiložení prstu na snímací plochu senzoru, bez pohybu prstu po ploše. Jde o poměrně jednoduchou metodu. Nevýhodou může být nepřiměřený tlak uživatele a tím možnost poškození zařízení. Je zde také pravděpodobnost špatného umístění prstu na senzor, např. pod jiným úhlem. Senzory jsou náchylné na znečištění.[3]

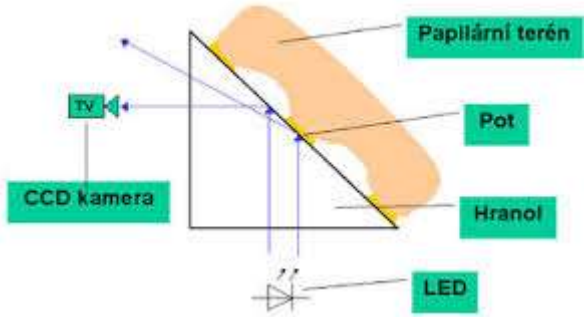
3.1.3. Snímání šablonováním

Jedná se o metodu, kdy uživatel přejíždí prstem po snímací ploše senzoru. Senzor snímá a skládá obraz otisku pomocí tvorby tzv. pásů. [3]

3.2. Metody snímání otisku prstu

3.2.1. Optická metoda

Optický princip je založen na vysílání světelného paprsku ze zdroje světla (LED). Paprsek osvětluje prst, který se dotýká snímací plochy senzoru. Množství odráženého světla závisí na hloubce papilárních linií (brázdy a hřebeny). Hlubší struktury, brázdy**,** odrážejí méně světla. Odražený světelný tok snímají CCD prvky (Charge Coupled Device). Papilární linie odrážejí více světla, proto je CCD senzor nastaven především na snímání odrazu od těchto vyvýšenin. Na odraz má vliv i znečištění. Především potně-tukový výměšek, příp. špína a jiné znečištění mezi sklem a pokožkou. Na senzoru mohou ulpívat zbytky pokožky, které pak dále znečisťují a zkreslují výsledky snímání. 3D optické senzory využívají bezkontaktní metody. Světelný paprsek umožňuje snímání na vzdálenost 3-5 cm. Výhodou je eliminace znečistění snímací plochy senzoru. [1][2]



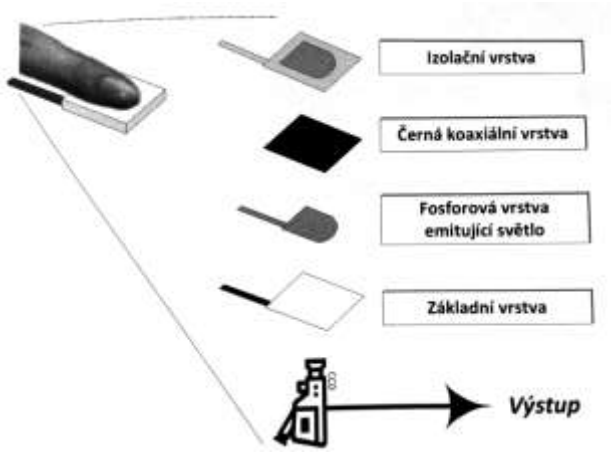
Obrázek 6: Optická metoda snímání [19]

3.2.2. Tlaková metoda

Tyto senzory snímají změny tlaku vlivem přiložení papilárních linií na povrch senzoru. Senzor je tvořen třemi vrstvami. Povrch senzoru je tvořen elastickým, piezoelektrickým materiálem (piezoelektrické krystaly). Prostřední vrstva je nevodivá, a spodní vrstva je opět elektrovodivá. Při dotyku prstu se tlak přenese přes nevodivou část tak, že se elektrovodivé vrstvy dotknou. Tato plocha převede tlakovou sílu na elektrický signál. Tímto je vytvořen daktyloskopický obraz. Papilární linie vyvolávají větší tlakové působení oproti brázdám, které mají nižší tlak. Výhody tlakové metody: tento typ senzoru je odolný vůči vlhkosti prostředí oproti jiným typům senzoru. Tudíž je schopen snímat i vlhké popř. suché otisky prstů.[1][2][3]

3.2.3. Opto-elektronická metoda

Senzor pracující na této metodě je složen z několika vrstev. Horní vrstva, která je v kontaktu s kůží, je schopna emitovat světlo po dotyku (polymer TFT). Pod vrstvou, dotýkající se prstu, je fosforová část, která osvětluje celou plochu prstu. Světlo dále zachytí skleněná vrstva, hustě osídlena fotodiodami. Fotodiody (nebo také senzory CCD) převedou světelný impuls na elektrický, čímž vytvoří elektronický obraz prstu.



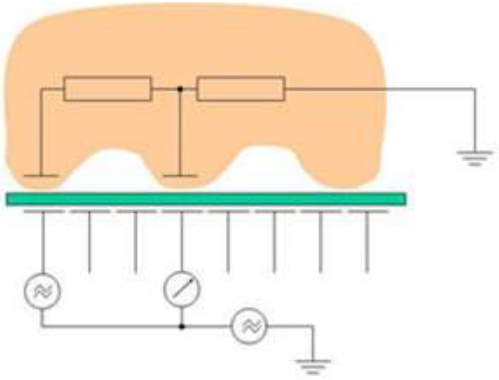
Obrázek 7: Opto-elektronická metoda snímání [1]

Mezi nevýhody opět řadíme možnost znečištění snímací plochy senzoru, pravděpodobnost ulpění zbytku pokožky na snímací ploše senzoru. Mezi výhody patří odolnost proti statickým výbojům a odolnost proti vlivu okolního prostředí, vysoká kvalita.[1][2]

3.2.4. Kapacitní senzory

Tento druh senzoru byl navržen pro snímání změny elektrické kapacity vlivem přiložení prstu na plochu snímače. Kapacitní senzor je složen z většího počtu vodivých ploch (maticově uspořádány), vzájemně odizolovaných (vrstvou napařeného nevodivého oxidu křemičitého). Jemnost těchto ploch je vyšší než jemnost papilárních linií. Při přiložení prstu na snímací plochu se vlivem vyvýšených papilárních linií přemosťují jednotlivé vodivé plošky. Brázdy se chovají jako izolant. Měří se napětí a jednotlivé kapacitní úbytky mezi vodivými plochami. Vodivé plochy, tedy elektrody, převádějí kapacitně otisk prstu na digitální signál. Výsledkem je digitalizovaný obraz papilární kresby.

Mezi výhody řadíme: malý rozměr, jednoduchý princip funkce, vysoká kvalita. Nevýhodami jsou: krátká životnost, neodolnost vůči statické elektřině, nutnost výměny snímače zhruba po 3 letech, citlivost na elektromagnetický šum, citlivost na znečištění pokožky, která může vést ke změně vodivosti lidské kůže. Také je zde problém s tzv. suchými prsty.[1][2][3]

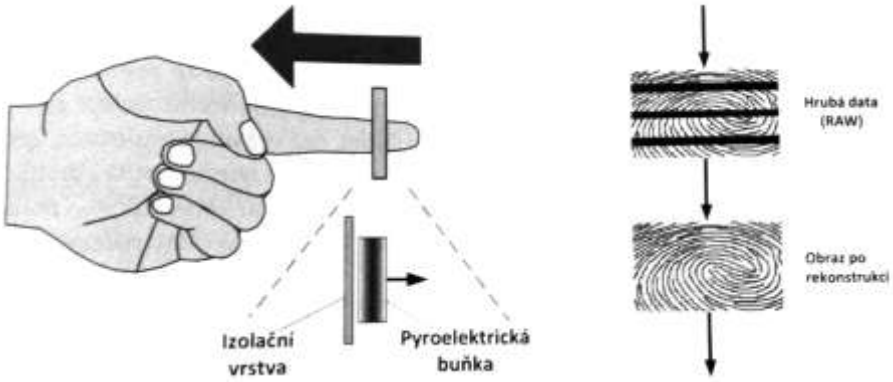


Obrázek 8: Kapacitní metoda snímání [19]

3.2.5. Tepelná metoda

Tato metoda je založena na tepelném záření. Čidlo je schopno rozeznat teplotní rozdíly mezi papilárními strukturami, které se dotýkají snímací plochy. Větší vyzařování tepelné energie mají papilární linie. Brázdy vyzařují nižší úroveň záření, protože jsou více vzdáleny od povrchu snímací plochy. Aby byl získán otisk prstu, je nutné prstem přejíždět po snímači. Otisk je získán ve formátu digitálních pásů. Z pásů je složen závěrečný otisk. Díky teplotě, která je dobrým ukazatelem stavu člověka, je možno také zjistit zda se jedná o prst patřící živé osobě. Výhodou tedy je, že částečně dokáže eliminovat pokusy o podvod s neživými otisky. Ovšem příkladem je zimní období, kdy nemusí být tento postup zcela vhodný z hlediska rozdílné teploty končetiny.

Mezi nevýhody je řazeno: nízká kvalita, problém algoritmů pro zpracování markantů, jiná část prstu v případě několikanásobného sejmutí otisku, špatná kvalita obrazu.[1][2][3]



Obrázek 9: Tepelná metoda snímání [1]

3.2.6. Ultrazvuková metoda

Senzory jsou založeny na podobném principu jako optické snímače. Na povrch prstu dopadá krátkovlnný svazek a odráží se od povrchu dle reliéfu papilárních linií a brázd. Snímány jsou zvukové vlny s vysokou frekvencí, řádově MHz. Princip této metody je přirovnáván k sonaru. Vlny jsou generovány zdrojem (vysílačem), který směřuje směrem ke snímané ploše. Vlny jsou pohlcovány přijímačem, který leží v rovině a je kolmý k vysílanému paprsku. Signál, který je vysílán, má velmi krátké impulsy v rozmezí 4-25 MHz. Odražené a deformované vlny jsou snímány senzorem, který má rotující hlavu. Deformované vlny vznikají díky netypické reakci na plastický povrch otisku prstu. Jedná se především o padělané otisky. Další variantou snímače je hustá síť snímacích čidel umístěných v rovině. Vyhodnocuje se vzájemný funkční vztah mezi odraženými a přijatými vlnami. Výsledkem je 3D odraz s vysokým kontrastem. Jako výhoda je brána vysoká přesnost 0,1 mm. Další výhodou je schopnost ultrazvukových vln proniknout do hlubší vrstvy kůže, čímž lze zabránit použití padělaných otisků. Podvrhy bývají zpravidla dvourozměrné. Tato metoda je nezávislá na čistotě prstů, vlhkosti otisků, či obroušení slabé vrstvy kůže. Výsledkem je obraz bez zkreslení. Vhodná i pro otisky dlaní.[1][3]

3.3. Parametry snímačů otisků prstů

U snímačů nás zajímají určité parametry. Jedním z nich je rozlišení, které se pohybuje od 250 dpi až po 1000 dpi. Nejběžnější je hodnota okolo 500 dpi. Další parametr je snímací plocha. Nejběžnější je velikost 0,7 cm x 0,7 cm pro přístupové systémy. Velikost 10 cm x 6 cm je využívána u daktyloskopických systémů, z důvodu užití rolovaného otisku prstu. Co se týče bitů, nejběžnější je pro odstíny šedé 8 bitů. Výjimečně hovoříme o 3 bitech. Dále ještě geometrická přesnost (zkreslení oproti skutečnosti) a kvalita obrazu.

Co se týče spolehlivosti a bezpečnosti snímačů, lze hovořit především o dvou parametrech, které jsou udávány u každého snímače. Řadíme zde míru chybného přijetí (FAR) a míru chybného odmítnutí (FRR). [1][2][3]

3.3.1. FAR

Míra chybného přijetí (FAR-False Accept Rate) je pravděpodobnost, kdy biometrický systém chybně vyhodnotí dva odlišné biometrické obrazy jako shodné. Dojde k selhání systému. Systém selže při odmítnutí možného útočníka. Tato chyba je udávána v procentech (%). [1][2][3]

3.3.2. FRR

Míra chybného odmítnutí (FRR- False Reject Rate) je pravděpodobnost, kdy biometrický systém chybně vyhodnotí dva biometrické obrazy od stejné osoby jako neshodné. Dojde selhání systému při přijetí oprávněného uživatele. Tato chyba je udávána v procentech (%).[1][2][3]

3.3.3. Searching time

Mezi další parametry senzorů patří Searching time. Jde o významný faktor v případě identifikace (1:N), neboli vyhledávání otisku v databázi. Jde tedy o čas, za který je šablona vyhledána v databázi. Tento parametr je udáván v sekundách (např. Searching time < 1s). [1][2][3]

3.3.4. Verification Time

Jedná se o dobu, za kterou senzor vyhodnotí, zda se šablona prstu na vstupu shoduje s šablonou povolující přístup do systému. Tímto potvrdí či nepotvrdí shodu, a také přístup do systému. Tento parametr je udáván v sekundách. [1][2][3]

3.3.5. Imaging time

Také zvaný Image acquiring time je čas pořízení obrázku. Parametr udáván v sekundách podobně jako u Searching time. [1][2][3]

3.3.6. Další vlastnosti

Jako další jsou zde řazeny elektrické a fyzikální vlastnosti senzoru. Napájecí napětí, pracovní proud, maximální proud, vhodná teplota a vlhkost okolního prostředí pro správnou funkci.

Dále jsou udávány Bezpečnostní úrovně (Security level). Většinou se jedná o pět úrovní (může být i více či méně). Na jednotlivých úrovních jsou nastaveny různé hodnoty jednotlivých chyb a odchylek. Např. na střední úrovni je vyrovnané nastavení chyb FAR a FRR. Při udávání hodnot míry chybného přijetí a míry chybného odmítnutí, bývají udávány i bezpečnostní úrovně, pro něž jsou hodnoty těchto chyb platné. [1][2][3][11]

3.4. Detekce živosti otisku prstu

Detekce živosti při snímání otisků prstů tvoří významnou část procesu. Otisky prstů zanechává člověk prakticky kdekoli. Na každém objektu, kterého se lidé dotknou, zůstávají otisky prstů. Z těchto objektů je pak snadné otisky sejmout. Pro toto získávání otisků prstů existuje velké množství metod. Je zde zahrnuta široká škála daktyloskopických prášků, speciální napařovací a napravovací techniky. Tyto metody dokážou efektivně zviditelnit otisk, který je pak sejmut. Ten může být dále používán, či kopírován. Výroba falešného otisku není náročná, lze ji zvládnout i v domácích podmínkách. Samozřejmě tyto metody slouží i v kriminalistice, ale z velké části i k zneužití a páchání trestné činnosti. Detekce živosti je poměrně důležitá, ovšem u čidel běžně dostupných na českém či zahraničním trhu se tato vlastnost vyskytuje zcela výjimečně.

Principů detekce živosti u otisků prstů je velké množství. V poslední době se na trhu vyskytují nové technologie. Jsou zde metody poměrně jednoduché a také cenově dostupné, stejně tak jako metody náročnější na realizaci, ovšem o to více funkčně spolehlivé.[3][1][2][4][9]

3.5. Metody detekce živosti otisku prstu

3.5.1. Detekce potu

Jako velká část lidského těla, i pokožka prstu je zásobena potními žlázami. Tato metoda souvisí s detekcí činnosti potních pórů. Přiložení prstu na plochu senzoru je nutné po dobu několika sekund, aby byl senzor schopen registrace aktivity potních žláz.

3.5.2. Spektroskopické vlastnosti

Jedná se o metodu pracující na základě multispektrálních vlastností pokožky. Princip metody spočívá v osvětlení povrchu snímaného prstu s různými vlnovými délkami. Díky schopnosti tkáně, částečně pohlcovat záření či částečnému odrazu od struktur kůže, je možno využít tuto metodu. Dále je zde fakt, že kůže každého jedince reaguje mírně odlišně. Ovšem tento jev není zcela dostatečný. Tento padělek může být například nalepen. Určení padělku díky schopnosti různě pohlcovat záření.

3.5.3. Ultrazvuková technologie

Tato metoda využívá vlastnosti kůže, díky které ultrazvukové vlny proniknou pod povrch. Ultrazvukové vlny se při průchodu prostředím lámou a odrážejí. Při průchodu živým prstem, mají vlny svou specifickou odezvu. Když se tato odezva neshoduje, jde s největší pravděpodobností o padělek.

3.5.4. Fyzické vlastnosti

Fyzické vlastnosti lidského těla jsou nejjednodušší metody při získávání informace ohledně živosti prstu. Na druhé straně je zde také velká pravděpodobnost, že tyto údaje nebudou zcela správné. Tyto vlastnosti mohou být významně ovlivněny podmínkami okolního prostředí, psychickou či fyzickou kondicí jednice. V důsledku tohoto faktu není možno většinu z těchto parametrů použít.

Patří zde například teplota, reakce na teplý či studený podnět, změny při přítlaku, elektrické vlastnosti kůže, bioimpedance, aktivita srdce neboli pulz, oxidace krve, měření krevního tlaku. Je možno použít i specifická řešení, např. kombinaci některých z těchto faktorů.

3.6. Přenositelnost dat

Existují biometrické systémy, které sbírají data jen z jednoho místa (senzoru). Ovšem na druhé straně existují aplikace, které shromažďují data z mnoha míst. Popřípadě jsou data stahována z jednoho místa, ale k jejich úpravě či skladování dochází v jiném prostředí. Proto je nutné, tento proces přenosu zabezpečit, aby nedošlo ke ztrátě kvality získaného materiálu.

Protože mají biometrická data velký objem, jsou před přenosem komprimována. Po přenosu dochází k dekomprimaci, aby bylo možné se získanými materiály pracovat. Tento proces způsobuje ztrátu kvality dekomprimovaného signálu. Použité kompresní algoritmy záleží také na druhu

biometrické vlastnosti, kterou snímáme. Proto jsou hledány takové metody, které by kvalitu získaného materiálnu ovlivnily co nejméně. Aby byly biometrické systémy co nejvíce otevřené a mohly si vyměňovat data s ostatními aplikacemi biometrické sféry, je nutné komprimační, dekomprimační přenosové protokoly standardizovat.[20][7][6][2]

4. Zpracování obrazu

Proces zpracování a rozpoznávání obrazů reálného světa dělíme do několika základních kroků. Toto dělení není zcela jednoznačné, a v různé literatuře může být odlišné. Konkrétní aplikace postupu je individuální. Dnes se nejčastěji užívá digitální zpracování obrazu. Možná jsou i zpracování optická a analogová. Posloupnost základních kroků: snímání a digitalizace obrazu, předzpracování, segmentace obrazu, popis objektů, klasifikace.[8][5][17]

Prvním krokem procesu je získání obrazu reálného světa, následuje převod do digitální formy, aby bylo možné obraz zpracovat v počítači či jiném systému. [8][5][17]

4.1. Postup zpracování obrazu

4.1.1. Snímání obrazu

Jedná se o převod optické veličiny na elektrický signál, který je spojitý v čase i úrovni. Na výsledný obraz má vliv mnoho faktorů, např. ozáření snímaného objektu, poloha objektu k snímači. Vstupní informace pochází z kamery či scanneru. Jsou to veličiny jako intenzita rentgenového záření, ultrazvuk či tepelné záření.[17][5]

4.1.2. Digitalizace

Následuje převod spojitého analogového signálu na digitální signál. Tento jev je nazýván digitalizace. Spojitý signál je prvně vzorkován, jde o stanovení jeho velikosti v pravidelných časových intervalech. Interval má poměr ke spojitému signálu. Posloupnost získaných hodnot se dále kóduje. Digitální signál vytvoří posloupnost číselných údajů o určitých vlastnostech, v případě obrazu je řeč o pixelech. [17][15][16]

4.1.3. Předzpracování obrazu

Po úspěšném snímání obrazu a jeho digitalizaci následuje předzpracování. Děje se tak v případě, kdy je obraz zkreslen, např. špatným průběhem snímání. Řadíme zde tyto základní metody předzpracování: jasové a geometrické transformace, filtrace a ostření. [17][15][16]

4.1.4. Segmentace

Tato část patří mezi nejnáročnější. Jedná se o analýzu obrazu vedoucí k nalezení objektů (body zájmu v dalším zpracování). Cílem segmentace je rozdělení obrazu do objektů reálného světa. [17][15][16]

4.1.5. Popis objektů

Dalším krokem je popis obrazu a popis nalezených objektů v segmentaci. Existují dva základní postupy popisu, kvantitativní a kvalitativní. Kvantitativní postup řeší popis obrazu pomocí

číselných charakteristik, např. velikost objektu či množství objektů apod. Kvalitativní popis charakterizuje relace mezi objekty a z toho vyplývající tvarové vlastnosti. [17][15]

4.1.6. Klasifikace

Jedná se o zařazení objektů obrazu do předem známých tříd. Metody klasifikace objektů se dělí do dvou základních skupin. A to příznakové a strukturální rozpoznávání. Příznaková metoda využívá příznaky, tedy skupinu číselných charakteristik objektu. Strukturální metoda využívá kvalitativních popisů objektů. [17]

4.2. Vlastnosti obrazu

Digitální obraz zodpovídá za obrazovou informaci v digitální paměti. Díky svým vlastnostem je digitální obraz kvantován. Dělen na malé části. Tyto části jsou pixely, které mají jen jednu hodnotu jasu. Jas pixelu je informace, která odpovídá svítivosti plošky reálného obrazu. Tato plocha je promítnuta v příslušném pixelu. Nulovou svítivostí je charakterizována černá barva. V paměti počítače je zapsána jako 0. Bílá barva je nejvyšším použitelným číslem. V případě černobílého obrazu je tedy pro bílou přiřazena 1. Jde tedy o jednobitový obraz. V současných biometrických aplikacích je možno nastavit typ výstupu, např. až do 254 bitů.[5]

Nejvyšší použitelná hodnota jasu podává informace o schopnosti dané reprezentace obrazu v paměti počítače. Tato schopnost rozeznává různé úrovně jasu. Hodnota čísla, které je odpovídající pro tuto úroveň, je zvána bitová hloubka obrazu. Není obvykle uváděno vlastní číslo. Uvádí se počet bitů, které zabere v paměti číslo, definující jas jednoho pixelu.[17]

Bitová hloubka	Maximální jas	Komentář
1	2 (2^1)	Jen černá a bílá
2	4 (2^2)	
4	6 (2^4)	
8	256(2^8)	Běžně používané
24	16777216 (2^{24})	tzv. True color

Tabulka 1: Příklady používaných bitových hloubek. [12]

Tímto zápisem je charakterizována šablona otisku prstu. Vzhledem k tomuto faktu lze říci, že je možno porovnávat šablony senzorů různého typu. Pokud jsou šablony v tomto formátu. Musí být brány v potaz komprimační a dekomprimační procesy. (3.6)

Výstupním formátem zpracovaných dat se jako obrazový standard obvykle využívá formát JPEG pro zpracování lidských tváří a formát WSQ (Wavelet Transfroms/Scalar Quantisation). [2] Je

možné docílit jiných formátů například JPG či BMP a další standardní formáty. Tohoto cíle, a samozřejmě i vytvoření dalších šablon, lze docílit díky správnému naprogramování s užitím různorodých algoritmů. 17]

4.3. Postup zpracování a rozpoznávání otisků prstů

Prvním krokem je získání snímku otisku prstu. Je nasnímán vstupní obraz, dále je předzpracován a dochází k extrakci papilárních linií. Takto je docíleno vhodného popisu průběhu papilárních linií.

Je získán otisk prstu ze snímače či jiné předlohy. Vstupní obraz je zahlcen velkým množstvím šumu. Toto se dále upravuje. Nutné rozeznávat různé typy otisků prstů. Dále důležité brát v potaz znečištění otisku, poranění prstu, kontrola živosti apod. V jednotlivých bodech obrazu se vypočte směr papilárních linií z okolí. Vypočte se pole orientací pro každý bod snímku. Dále dochází k převedení na blokové pole orientací. Toto pole je namapováno na původní snímek. Následující krokem je extrakce papilárních linií do černobílé formy, která probíhá díky dalším úpravám a binarizaci neboli prahováním. Toto probíhá tak, že pro jednotlivé části obrazu, který je rozdělen na bloky 8x8 a 8x4 jsou vypočítány průměrné hodnoty úrovně šedé v této oblasti. Ztenčení papilárních linií je další krok. Při extrakci měli papilární linie různé šířky, proto je nyní provedeno ztenčení na tloušťku 1 bod. Dále dochází k detekci a extrakci markantů. Hledají se dva základní typy markantů a to ukončení papilární linie a vidlička. Ostatní druhy markantů jsou kombinací dvou zmíněných typů. Provádí se součet bodů v okolí. Pokud je součet roven 2, jde o ukončení. Pokud je součet roven 3, jde o vidličku. Ke každému markantu jsou ukládány další údaje. Je ukládána pozice markantu (popis pomocí souřadnic x a y), typ markantu (ukončení či vidlička), gradient (orientace, sklon papilární linie). [1] [3][4][5]

4.4. Metody zpracování otisků prstů

Do této oblasti jsou zařazeny tři hlavní typy. Metoda založená na markantech, metoda založená na korelaci a metoda založená na vlastnostech papilárních linií.

4.4.1. Metoda založená na markantech

Metoda založená na markantech je nejčastěji používané zpracování. Rovněž označována technikou založenou na specifických rysech, oblastech zájmu. Dochází ke zjištění a poté k extrakci množin markantů z obou porovnávaných otisků. Tyto množiny se porovnávají a hledá se většinou určitý počet markantů nacházejících se na stejné pozici. Dále také typy a umístění charakteristických bodů. Jádro, delta a tvar papilárních linií mezi spárovanými body singularity. Tyto získané výsledky jsou použity pro klasifikaci do náležitých tříd. [3]

4.4.2. Metoda založená na korelaci

Metoda založená na korelaci bývá označována jako obrazová technika. Korelace je algoritmus, který umožňuje vzájemně srovnávat posloupnosti vzorků. Porovnává umístění vztažných

bodů v otisku prstu. Tento systém vybere šablonu, která odpovídá prvnímu otisku prstu, pak další šablony odpovídá druhé otisku prstu, a to provádí jeden přes druhý. Při identifikaci provádí tak dlouho, dokud nenajde shodu. Při verifikace porovnává jen s požadovaným uživatelem. Při použití této metody, a to i tisky nízké kvality může být vyhodnocena přesně. Šablony dvou obrázků otisků prstů jsou položeny na sebe. Další částí je výpočet korelace mezi odpovídajícími pixely pro různé pozice (různé posunutí a natočení). [4][5]

4.4.3. Metody založené na vlastnostech papilárních linií

Klíčem této metody jsou charakteristické vlastnosti papilárních linií. Porovnávají se tvary papilárních linií, jejich hustotu rozložení na snímané ploše. Tento postup bývá také nazýván hybridní. Metoda kombinuje vybrané prvky obou předchozích postupů. [6][3]

5. Návrh praktické části bakalářské práce

Cílem práce je vytvořit hardware a software, který potvrdí shodu z nasnímaného otisku s referenčním otiskem. Čili vyhledá údaje majitele nasnímaného otisku v databázi systému. Pro tuto část je tudíž třeba vybrat správný senzor otisku prstu, díky němuž bude možno zrekonstruovat plnohodnotný hardware. Další části je napsat program, který porovná či rozezná zadávané otisky.

5.1. Výběr senzoru otisku prstu

Pro tuto práci bude využit senzor se statickým snímáním. Po prvotním průzkumu českého i zahraničního trhu jsem se zaměřila na optické a kapacitní snímače otisku prstu. Nutno podotknout, že český trh týkající se této problematiky je poměrně chudý. Lze zde nalézt především hotové různorodé biometrické systémy. Tyto systémy již obsahují zakomponované hardwarové i softwarové prostředí.

Při výběru čidla byly brány v potaz tyto základní parametry: komunikační rozhraní, dostupnost, FAR, FRR, vybavení, detekce živosti a také cenová dostupnost. (3.3.) Co se týče komunikačního rozhraní, tedy připojení snímače k počítači, prioritní bylo rozhraní UART nebo USB. Dostupnost senzoru byla brána především z časového hlediska. Dodací doba se mnohdy pohybovala okolo 2 měsíců. Odchylky FAR a FRR, jsou míry chyb senzoru. Tedy míra chybného přijetí (FAR) a míra chybného odmítnutí (FRR). Průměrně se tyto hodnoty pohybují okolo FAR<0,001 % a FRR= 1%. Z hlediska vybavení se jedná o možnosti poskytnutí nějaké softwarové aplikace, vývojové sady či modulu výrobcem. Dále bylo bráno v potaz, zda je senzor schopen detekovat živost prstu. Což je u běžně dostupných senzorů vzácné.

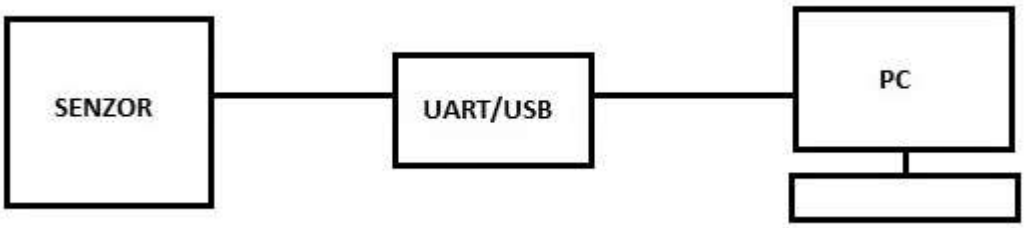
V níže přiložené tabulce jsou senzory, které se dostaly do užšího výběru na základě zmíněných základních parametrů. Po konzultaci s vedoucím práce byl vybrán senzor číslo čtyři.

	Název	**Cena [$]**	**FAR [%]**	**FRR [%]**	**Detekce životnosti**	**Obsah balení**	**Komunikační rozhraní**	**Poznámka**
1.	Čtečka otisku prstu	65,99	<0,001	<1,5	---	Senzor, module DPS	UART	Module SM-261
2.	Fingerprint sensor	49,95	<0,001	<1,0	---	Senzor, SW pro Windows, Arduino libary.	TTL Serial	
3.	Seeed Grove - Fingerprint Sensor	53,52	<0,001	<1,0	---	Senzor, Finge-rprint Sensor Library	UART (TTL Seriál); USB	Module AS601
4.	Optical Fingerprint Reader	39,94	<0,001	<0,1	---	Module Sensor	UART	Development Kit

Tabulka 2: Přehled vybraných senzorů otisků prstů

5.2. Propojení senzoru s počítačem

Vybraný senzor pracuje pomocí komunikačního rozhraní UART. Senzor je proto nutné propojit pomocí převodníku se sériovým rozhraním RS232. Proto bude použit převodník UART/USB. Převodník je pak dále propojen s počítačem. Soustavu je nutno doplnit softwarem. Data budou díky tomuto zapojení přenášena ze senzoru do počítače, kde můžou být dále zpracovávána. Komunikace se senzorem probíhá pomocí sériového rozhraní, tedy sériové linky.[24]



Obrázek 10: Schéma zapojení senzoru s PC

5.3. Parametry vybraného senzoru otisku prstu

Senzor komunikuje s počítačem pomocí sériové linky. Pro tuto komunikaci má senzor definované vlastnosti. Mezi základními údaji je definována BaudRate, tedy přenosová rychlost. Tento parametr je udáván v jednotkách bps (bits per second). Pro tento senzor se přenosová rychlost rovná 19200 bps. Dále přenos probíhá za účasti jednoho start bitu (rozběhový prvek přenosu) a jednoho stop bitu (závěrný prvek přenosu). Komunikace funguje prostřednictvím komunikačního protokolu. Ten se skládá z osmi bytů. [11][24]

Byte	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Command	0xF5	CMD	P1	P2	P3	0	CHK	0xF5
Response	0xF5	CMD	Q1	Q2	Q3	0	CHK	0xF5

Tabulka 3: Komunikační protokol senzoru otisku prstu [11]

První a poslední byte nese hodnotu F5. Převedeno do desítkové soustavy jako číslo 245. Druhý byte (CMD) definuje požadovaný příkaz (command) či odpověď (response). Pro jednotlivé operace existuje specifický komunikační protokol. Sedmý byte (CHK) definuje hodnotu checksum. Tato hodnota nese název kontrolní součet, či kontrolní byte. Jedná se o součet počtu bitů v přenosové části. Dochází tak k ověření, zda došel zpět stejný počet bitů, popř. bytů. Pro tento senzor lze kontrolní součet vypočítat pomocí logické funkce XOR neboli exkluzivní součet. Tento součet provádíme od druhého bytu až k šestému. Výsledek se objeví na sedmé pozici komunikačního protokolu. Na pozici pátého bytu (Q3) je vrácena efektivní provozní informace. Jedná se o správnost procesu, a informaci ohledně uživatelů systému. [11]

CMD: Command/ response type	
P1, P2, P3: Command type (příkaz)	
Q1, Q2, Q3: Response type (odpověď)	
Q3 užívána především jako návrat efektivní operační informace, následují příslušné hodnoty:	
○ #define ACK_SUCCESS **0x00**	Operace proběhla úspěšně.
○ #define ACK_FAIL **0x01**	Operace proběhla neúspěšně.
○ #define ACK_FULL **0x04**	Databáze otisků prstů je plná.
○ #define ACK_NOUSER **0x05**	Nenalezen takový uživatel.
○ #define ACK_USER_EXIST **0x07**	Uživatel již existuje.
○ #define ACK_TIMEOUT **0x08**	Akviziční timeout.

Tabulka 4: Definice bytů komunikačního protokolu a jejich informační hodnota [11]

Pro uskutečnění komunikace senzoru s počítačem jsem využila přiložený datasheet. Definuje již výše zmíněné parametry komunikace a také funkce, které umí senzor provést.

Z manuálu senzoru vychází několik předem nadefinovaných funkcí. Je zde možno nalézt vykreslení otisku prstu, uložení nového uživatele, porovnání otisku neboli verifikace, vyhledávání otisku uživatele, tedy identifikace. Dále je možno jednotlivé uživatele smazat. Dále u každého uživatele je možno nastavit oprávnění. Toto oprávnění je možno využít k omezení přístupu do určitých částí biometrického systému. [11]

5.4. Algoritmy využité pro tvorbu programu

Pro tvorbu programu jsem využila přiložené algoritmy jednotlivých funkcí. Součástí je také algoritmus pro vymazání vybraného uživatele či vymazání všech uživatelů. Tento algoritmus funguje jednodušeji a to na principu jediného příkazu a následné odpovědi.

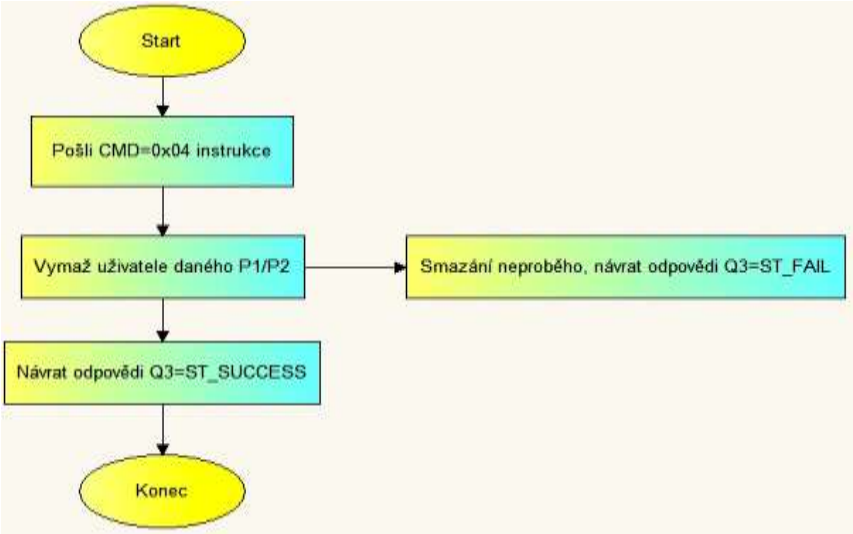


Diagram 1: Algoritmus pro vymazání vybraného uživatele [11]

Další je algoritmus slouží pro vymazání všech uživatelů z databáze. Tento algoritmus funguje taktéž jednoduše a to na principu jediného příkazu. Následné odpověď značí, zda smazání proběhlo (Q3=ST_SUCCESS) či neproběhlo (Q3=ST_FAIL).

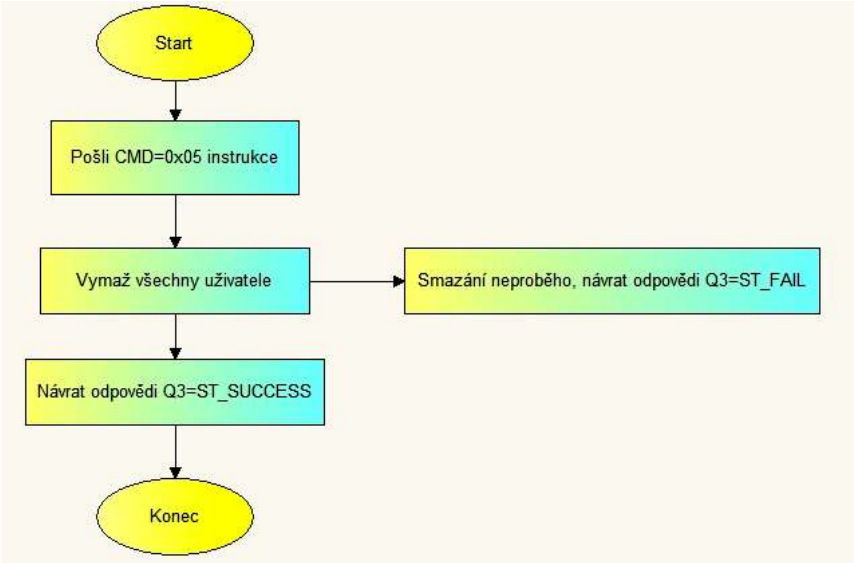


Diagram 2: Algoritmus pro vymazání všech uživatelů [11]

Algoritmus pro vytvoření nového uživatele do databáze senzoru probíhá ve třech krocích. Jednotlivě po sobě jsou posílány příkazy, které dostávají příslušnou odpověď. V případě, že všechny tři části proběhnout v pořádku, je uživatel uložen do databáze senzoru.

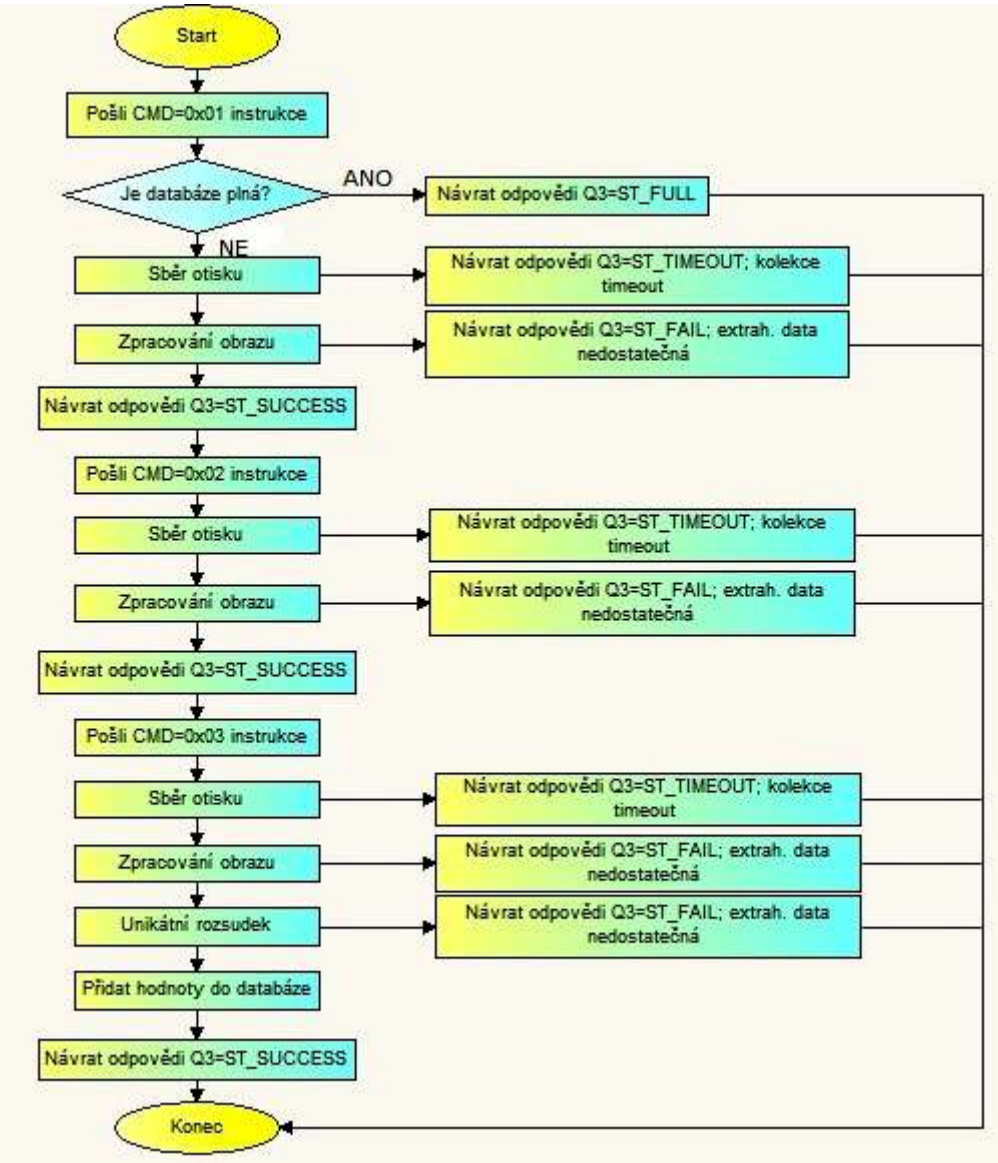


Diagram 3: Algoritmus pro přidání nového uživatele [11]

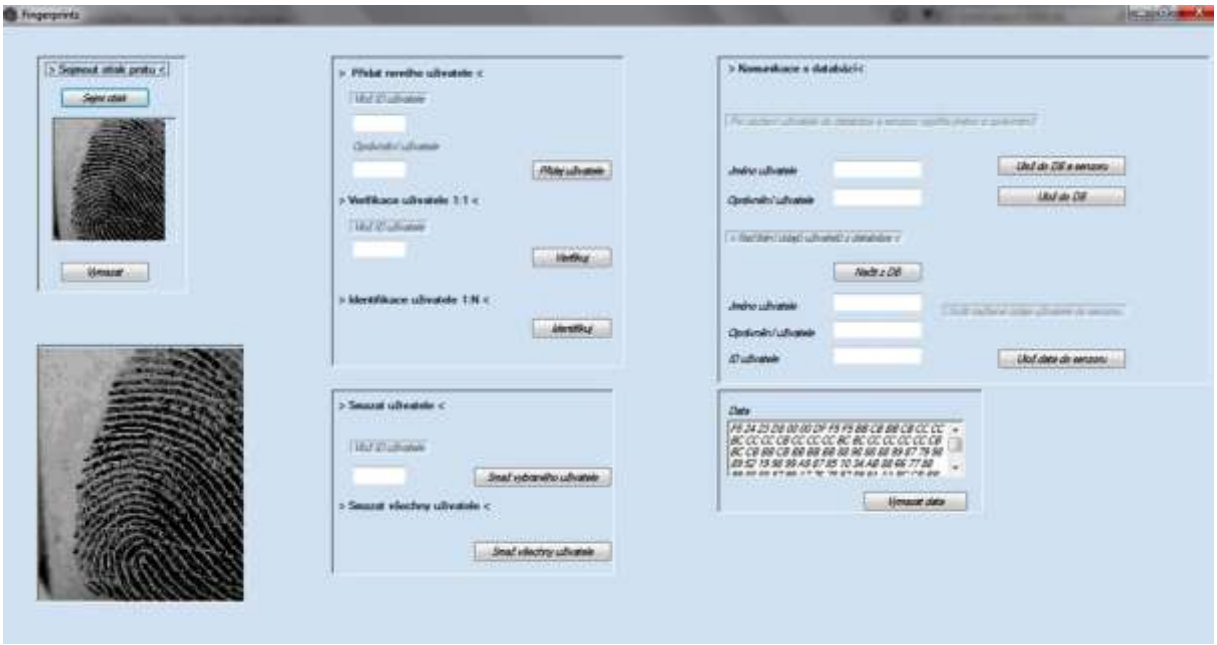
5.5. Software

Do této části zahrnuji výše uvedený software pro propojení senzoru s počítačem. Program bude sestaven pomocí jazyka C#. Součást programu tvoří rekognice a identifikace uživatele. Program je tvořen ve vývojovém prostředí Microsoft Visual Studio 2013. [12][13][14]

C# je vysokoúrovňový objektově orientovaný programovací jazyk vyvinutý firmou Microsoft zároveň s platformou .NET Framework. Společnost Microsoft založila C# na již existujících jazycích C++ a Java. Tento jazyk lze použít k tvorbě databázových programů, webových aplikací a stránek, webových služeb, formulářových aplikací ve Windows, softwaru pro mobilní zařízení apod.[12][13][14]

Senzor komunikuje s počítačem pomocí sériové linky. Proto jsem vytvořila program, který všechny údaje a parametry zahrnuje, a je schopen využít možnosti senzoru. Všechny parametry a funkce jsou dále popsány. [14]

Pomocí třídy SerialPort jsem nastavila parametry pro komunikaci pomocí sériového rozhraní. Pomocí události *SerialDataReceivedEventHandler* došlo k přijetí dat skrz sériovou linku ze senzoru. Data, která program přijme, jsou typu byte. Po přijmutí 9187 bytů musí být data dále zpracována. Z dat musí být odebrána hlavičková data, startovní a koncový byte, hodnota checksum. Následně zůstanou pouze surová data, která reprezentují samotný otisk prstu. Tato data jsou možno pak vykreslena. To vidíme na obrázku 14 vlevo. Podle definice v manuálu, reprezentuje jeden byte 2 pixely. Vykresluje obrázek otisku o 140 řádcích. Každý řádek má 122 pixelů. Všechny tyto údaje jsou zahrnuty v kódu. Pro každý pixel existuje příslušná hodnota odstínů šedi. Kdybychom se hlavičkových dat, startovního a koncový bytu nezbavili, projevilo by se to chybou v obraze otisku.[11][12]



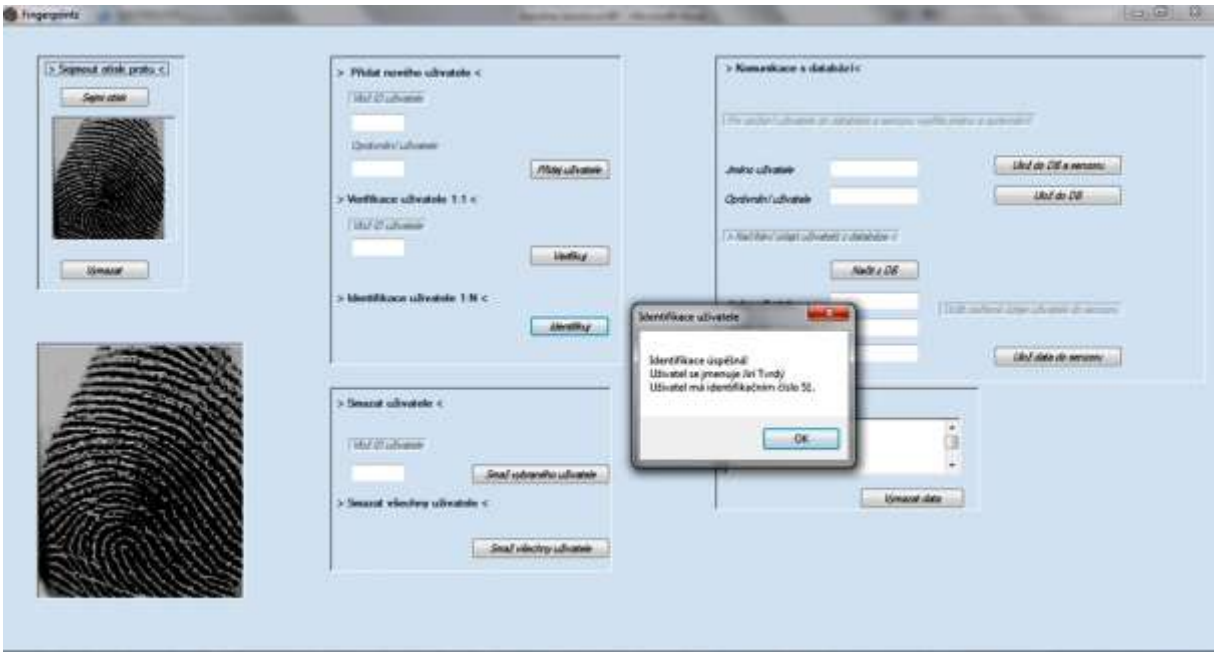
Obrázek 11: Vykreslení otisku prstu

V programu je součástí také identifikace a verifikace uživatele. Tyto operace probíhají pomocí rozpoznávání. Toto rozpoznávání funguje na principu korelace. Senzor vytvoří řetězec bytů, charakterizující otisk prstu. Když je hledán otisk v databázi, je snímaný otisk byte po byte srovnáván s referenčními otisky. Dokud není nalezena shoda. 4.4.2

Další obrázek ukazuje identifikaci uživatele. K tomuto úkolu jsem využila již zmíněnou funkci senzoru. Využívám funkci, kterou má senzor naprogramovanou pro identifikaci. Rozpoznávání 1:N tedy provádí samotný senzor. Senzor vytvoří řetězec bytů pro obraz otisku prstu. Když je hledán otisk v databázi, je snímaný otisk byte po byte srovnáván s referenčními otisky. Dokud není nalezen shodný uživatel. Systém vypíše identifikační číslo. V případě připojení k databázi MySql i jméno uživatele.

Byte	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Command	0xF5	0x0C	0	0	0	0	CHK	0xF5
Response	0xF5	0x0C	User ID 8-bit (vyšší priorita)	User ID 8-bit (nižší priorita)	ACK_SUCCESS ACK_FAIL ACK_TIMEOUT	0	CHK	0xF5

Tabulka 5: Komunikační protokol pro identifikaci uživatele [11]

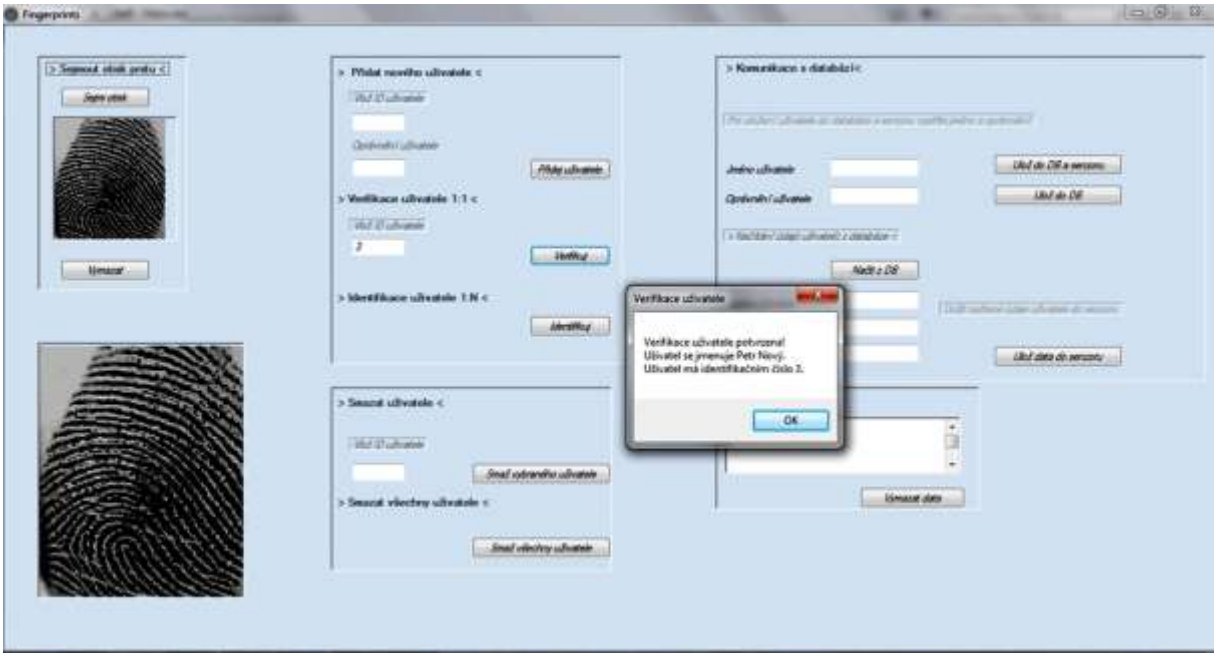


Obrázek 12: Identifikace uživatele

Obrázek 16 ukazuje verifikaci uživatele. K tomuto úkolu jsem využila již zmíněnou nadefinovanou funkci senzoru podle komunikačního protokolu v Tabulce 6. Využívám nadefinované příkazy a odpovědi dostupné u senzoru. Rozpoznávání 1:1 provádí samotný senzor.

Byte	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Command	0xF5	0x0B	User ID 8-bit (vyšší priorita)	User ID 8-bit (nižší priorita)	0	0	CHK	0xF5
Response	0xF5	0x0B	0	0	ACK_SUCCESS ACK_FAIL ACK_TIMEOUT	0	CHK	0xF5

Tabulka 6: Komunikační protokol verifikaci uživatele [11]



Obrázek 13: Verifikace uživatele

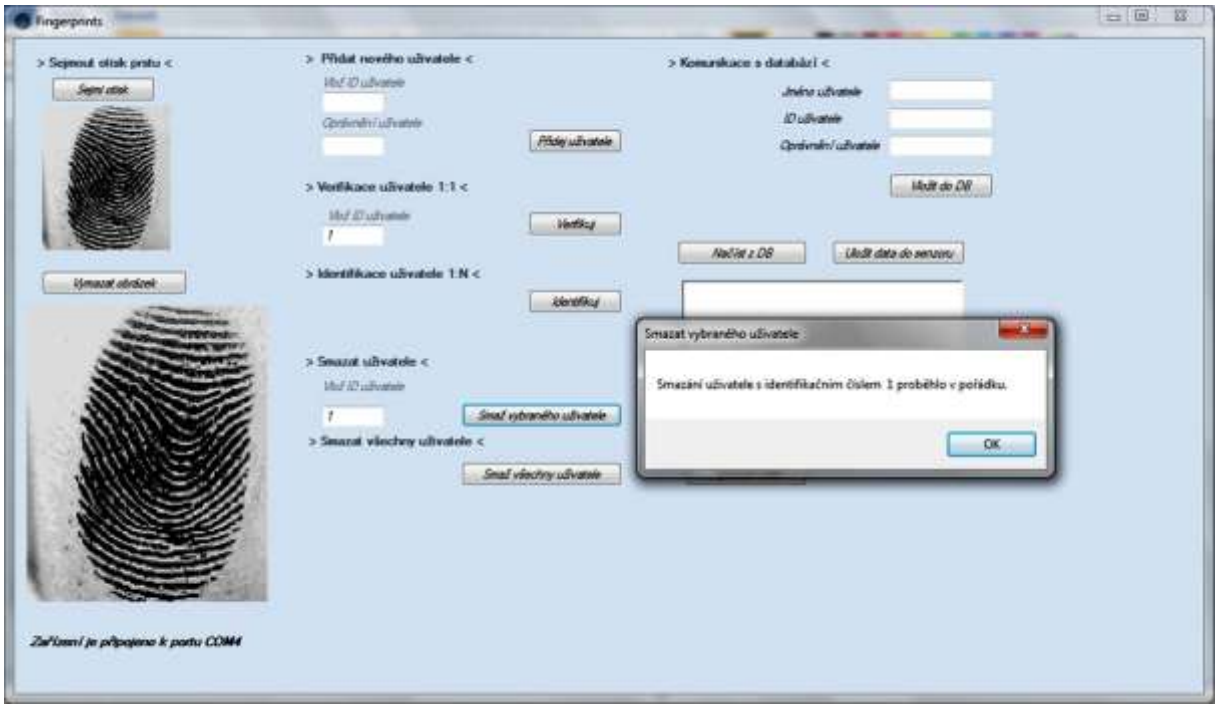
Jako další se v programu vyskytuje možnost smazat uživatele. A to buď jednoho vybraného podle jeho identifikačního čísla, nebo lze vymazat celou databázi uživatelů.

Byte	1	2	3	4	5	6	7	8
Command	0xF5	0x04	User ID 8-bit (vyšší priorita)	User ID 8-bit (nižší priorita)	0	0	CHK	0xF5
Response	0xF5	0x04	0	0	ACK_SUCCESS ACK_FAIL	0	CHK	0xF5

Tabulka 7: Komunikační protokol pro smazání vybraného uživatele [11]

Byte	1	2	3	4	5	6	7	8
Command	0xF5	0x05	0	0	0	0	CHK	0xF5
Response	0xF5	0x05	0	0	ACK_SUCCESS ACK_FAIL	0	CHK	0xF5

Tabulka 8: Komunikační protokol pro smazání všech uživatelů [11]

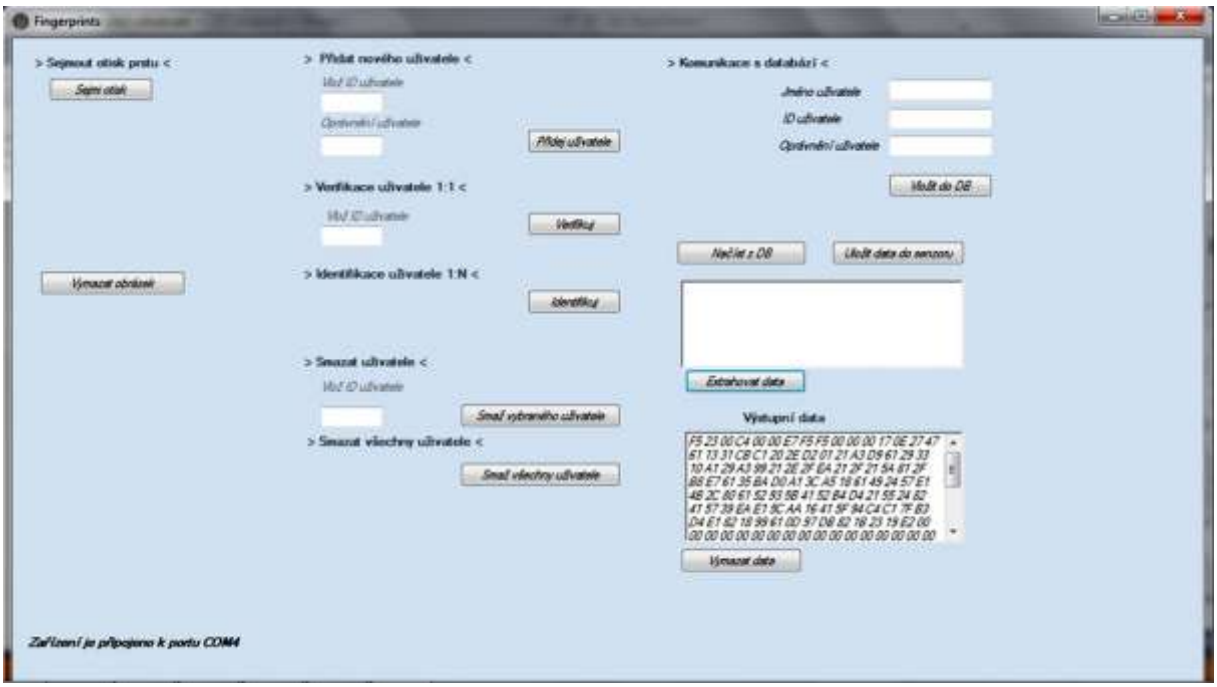


Obrázek 14: Smazání uživatele

Taktéž existuje funkce pro extrakci dat. Jsou to data reprezentující otisk prstu, ale jsou extrahovaná. Mají tedy menší objem. Tato data se dají zpětně uložit do senzoru pod zvoleným identifikačním číslem. Takto získaná data, která jsou upravena, ukládám do databáze. Úprava je nutná, protože extrahovaná data obsahují hlavičkovou informaci, které je nutná k extrakci. Tyto byty je nutno odstranit. Tedy hlavičková data (byty), startovní a koncový byte, hodnota checksum. Díky tomuto procesu zůstanou surová data charakterizující otisk prstu. Checksum, tedy kontrolní byte, se dopočítá podle funkce, ke které chci upravená extrahovaná data následně použít. 5.3

Byte	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Command	0xF5	0x23	0	0	0	0	CHK	0xF5
Response **(header)**	0xF5	0x23	Length 8bit (vyšší priorita)	Length 8bit (nižší priorita)	ACK_SUCCESS ACK_FAIL ACK_TIMEOUT	0	CHK	0xF5
Response **(packet)**	0xF5	0	0	0	Eigenvalues data	CHK	0xF5	

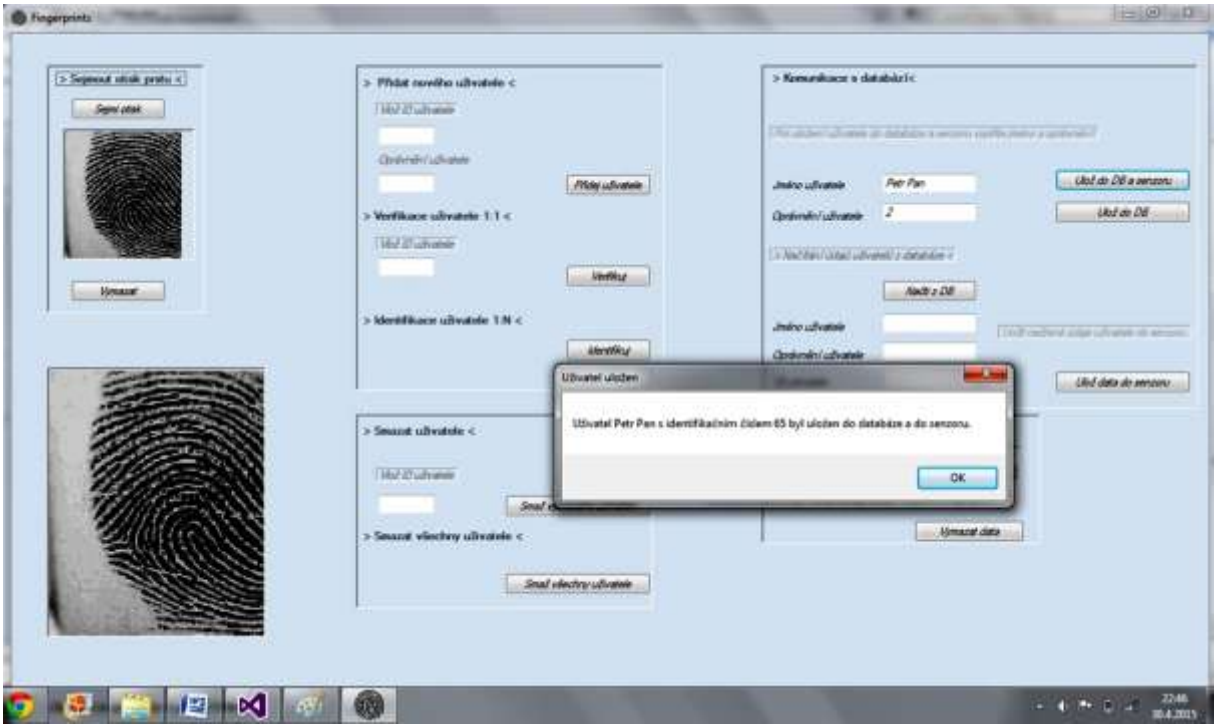
Tabulka 9: Komunikační protokol pro extrakci dat [11]



Obrázek 15: Extrakce dat (vpravo dole)

Následující funkce slouží k uložení extrahovaných dat do databáze a následně také do senzoru. Senzor extrahuje data, ta jsou pak dále upravena. Proto, abychom získali jen čisté data reprezentující

otisk prstu. Tyto data jsou pak uložena do databáze. Z databáze jsou načtena zpět do programu a pak uložena do senzoru. Schematicky je funkce popsaná na Diagramu 4.



Obrázek 16: Uložení otisku do databáze a senzoru

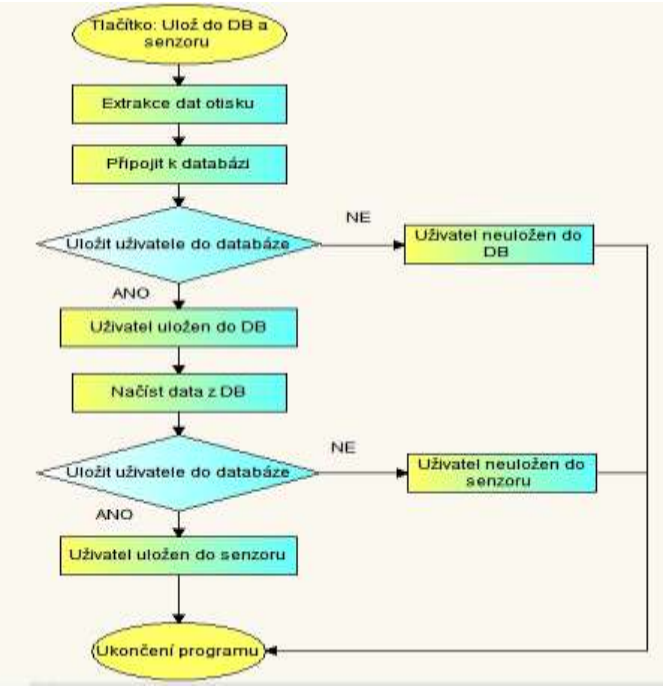


Diagram 4: Proces uložení dat

5.6. Komunikace s databází, přenos dat

K této bakalářské práci jsem vytvořila také databázi. Tuto databázi jsem vytvořila na serveru CPIT, (Vědecko-výzkumné laboratoře Vysoké školy báňské). Databáze je vytvořena pomocí aplikace phpMyAdmin. [22]

Aplikace phpMyAdmin je populární nástroj pro správu MySQL databáze. Rozhraní aplikace je plně lokalizováno do češtiny. MySQL databáze slouží k ukládání dat aplikací. Programový systém phpMyAdmin je nástroj napsaný v jazyce PHP. Tento jazyk umožňuje jednoduchou správu obsahu databáze MySQL a to prostřednictvím webového rozhraní. V této aplikaci je možno vytvářet/rušit databáze, vytvářet/upravovat/rušit tabulky, provádět SQL příkazy a spravovat klíče. Jedná se o jeden z nejpopulárnějších nástrojů pro správu databáze. Je k dispozici v 57 jazycích. [22][23]

Díky této aplikaci jsem si vytvořila databázi. Do této databáze ukládám data reprezentující otisk prstu. Ke každému otisku je uloženo identifikační číslo uživatele, jméno uživatele a jeho oprávnění v systému. Data uložená v databázi můžu různě zpracovávat. Prioritou pro mou práci je přenositelnost. Tedy přenést data charakterizující otisk prstu. Například uložení dat z databáze do senzoru. Nebo naopak načtení dat ze senzoru do databáze. Tato databáze má tedy sloužit jako prostředník pro přenos dat otisků prstů mezi více senzory. Jde tedy úložiště dat charakterizujících otisk prstu.

5.6.1. Databáze otisků prstů

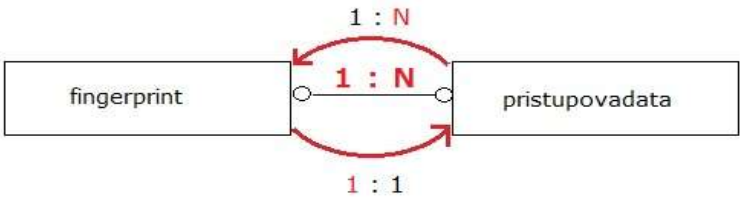
Po přidělení přístupu na server rc111 jsem v programu phpMyAdmin vytvořila databázi s názvem jan0389. V této databázi jsem vytvořila dvě tabulky. Tabulka *fingerprint* nese údaje o uživateli a data pro otisk prstu. Tabulka *pristupovadata* poskytuje údaje o zápisu uživatele do databáze.

fingerprint (id, jmeno, fingeprintdata, privilegelevel,stav)
pristupovadata (id, id_fingerprint, datetime)

Tabulka 10: Základní schéma tabulek databáze

V případě, že máme tabulky, musíme definovat relaci. Relace je něco, co vytváří vztah mezi danými objekty, v tomto případě tabulkami. Proto je nezbytné vyhledat jednotlivé vztahy mezi objekty (tabulkami) a následně určit správnou relaci. [21]

Podle vzájemného vztahu tedy určíme relaci, viz Obrázek 20. Vzniká mezi dvěma tabulkami, kde jedna hodnota primárního klíče v hlavní tabulce, odpovídá hodnotě pole v druhé tabulce. Typ pro tuto databázi je 1:N. Podle schématu přiloženého níže se jedná o tuto relaci. Protože jeden uživatel uložený do databáze má více záznamů v tabulce *pristupovadata*. A naopak, jeden záznam s údaji o uložení či přístupu v *pristupovadata*, může mít pouze jednoho uživatele v tab. *fingerprint*.[21]



Obrázek 17: Schéma relace tabulek [21][23]

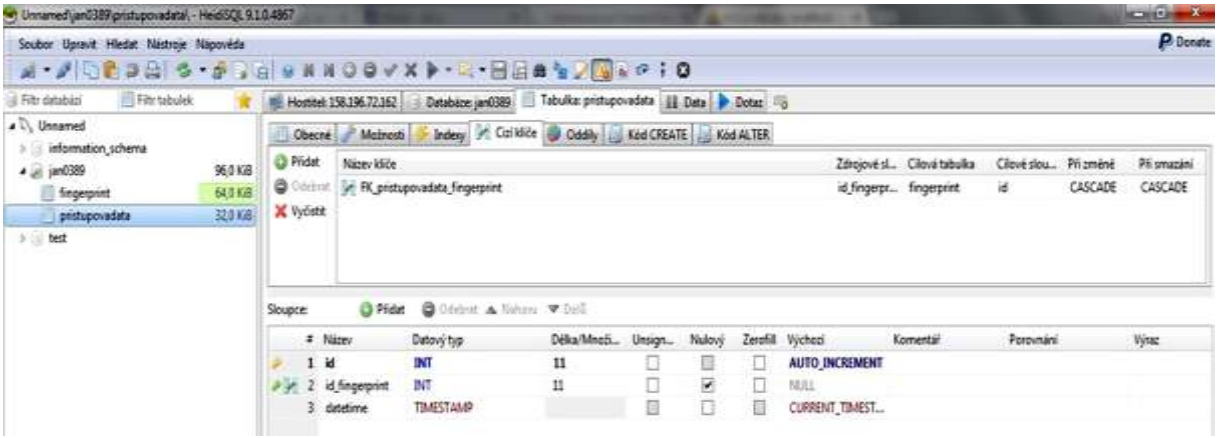
Obrázek 18: Struktura tabulky fingerprint

Obrázek 19: Struktura tabulky pristupovadata

Pro správnou definici relací a vzájemných vztahů je třeba definovat primární a cizí klíče. Primární klíč je pole, které identifikuje jednotlivé záznamy v databázové tabulce. Každé pole, které je součástí primárního klíče, má nenulovou hodnotu. Každá tabulka má mít definovaný právě jeden primární klíč. Cizí klíč realizuje vazbu. Relací 1:N se rozumí spojení, kde jeden záznam v hlavní tabulce obsahuje libovolný počet odpovídajících záznamů v podřízené tabulce.[21] [23]

U každé tabulky jsem nastavila primární klíč. V obou případech se jedná o *id* uživatele. Primární klíč jsem nastavila v prostředí phpMyAdmin. Cizí klíč ovšem takto nastavit nejde. K tomuto se využívá aplikace HeidiSQL.

HeidiSQL je prostředí určené pro práci s MySql databázemi. Umožňuje práci s tabulkami a jejich obsahy. Například prohlížení a úprava dat, vytváření a úprava tabulek, apod.



Obrázek 20: Definice cizího klíče pomocí HeidiSQL

Obrázek 21: Přehled zaznamenaných dat v phpMyAdmin

Na diagramech je schematicky zaznamenána komunikace programu pro identifikaci a verifikaci osob s databází otisků prstů. V programu jsou extrahována data charakterizující otisk, potom upravena a uložena do databáze. Každý uživatel dostane své identifikační číslo a je uložen pod svým jménem. Zároveň mu můžeme přiřadit oprávnění. To může sloužit například k omezení možností přístupu uživatele v systému. Naopak jdou data z databáze načíst do programu a následně uložit do senzoru. Tyto dvě funkce slouží především k přenosu dat mezi senzory. V rámci rozšířeného identifikačního systému.

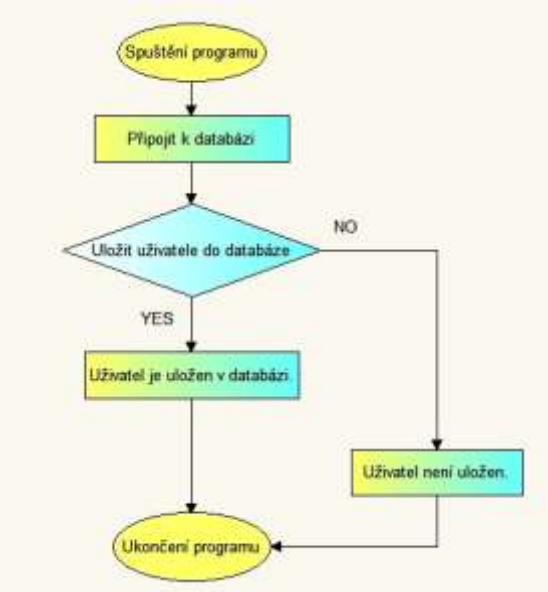


Diagram 5: Proces uložení dat

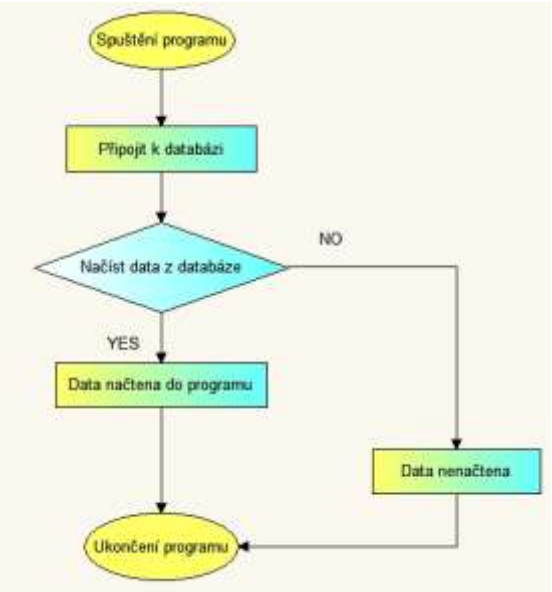


Diagram 6: Proces načtení dat

Databáze je zabezpečena přístupovým jménem a heslem. V databázi phpMyAdmin jsou uložena jak identifikační čísla a otisky prstů, tak i jména uživatelů. Toto je výhoda oproti senzoru. Protože do senzoru jdou uložit pouze identifikační čísla a otisky. Tudíž jméno uživatele se dozvíme až po připojení k databázi. Toto je výhoda, je zde menší pravděpodobnost zneužití osobních údajů osob třetí stranou.

Dále u každého uživatele je možno nastavit úroveň oprávnění. Tyto úrovně slouží v přístupových systémech k omezení vstupu do určitých oblastí. Takže, pro využití v praxi by bylo ještě potřeba definovat jednotlivé úrovně oprávnění. A podle potřeby je přidělit daným uživatelům.

Návod v příloze: I Návod Fingerprints

Zdrojový kód v příloze: III Fingerprints (Příloha na DVD

5.7. Fingerprint lock

Fingerprint lock je program sloužící k přístupu do systému. Využívá pouze identifikaci uživatele. V databázi jsou uloženy jen otisky uživatelů, kteří mají povolený přístup. Po potvrzení identifikace je povolen přístup danému uživateli. V opačném případě program nabídne opětovnou identifikaci. Podrobnější rozdělení přístupu uživatelů se dá specifikovat pomocí nastavení úrovně oprávnění přístupu. Proces identifikace zde funguje stejně jako v programu Fingeprints. 5.5Software Ve Fingerprint lock probíhá identifikace v cyklu neustále dokola. Nezávisle na ovládání příchozí účastníka. Viz. I - Návod k programu *Fingerprints*

Návod Fingerprint lock; Zdrojový kód v příloze: IV Fingerprint lock (Příloha na DVD

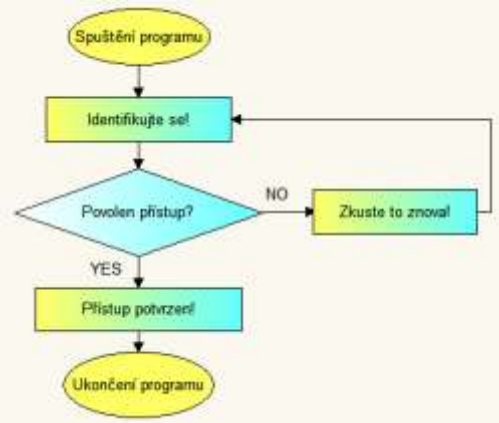


Diagram 7: Fingerprint lock, potvrzení přístupu

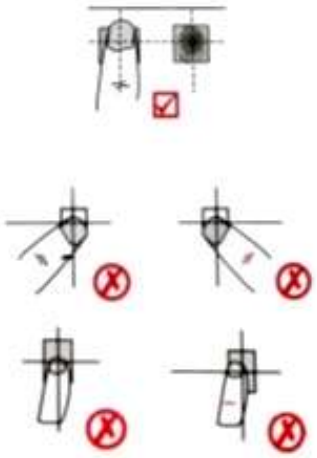
Tento program je možno využít jako zámek oprávněného vstupu do místnosti. Také je předpoklad využívání programu na napájecí stanice pro elektromobily na VŠB-TUO. Samotná implementace biometrického systému (senzoru a vytvořeného programu) je náplní jiné práce.

Obrázek 22: Fingerprint lock, potvrzení přístupu

5.8. Zhodnocení dosažených výsledků

5.8.1. Testování spolehlivosti senzoru

Spolehlivost senzoru je poměrně značně omezena na poloze při snímání otisku prstu. V případě, že je otisk dán do naprosto stejné polohy jako při snímání, je rozpoznání stoprocentní. Ovšem při změně polohy prstu je tato schopnost zcela omezena. Tato chyba je pravděpodobně způsobena metodou rozpoznávání. Protože senzor vytvoří šablonu otisku ve formě extrahovaných dat, tedy řetězce bytů. Pak snímanou šablonu porovnává s referenčními šablonami uloženými v databázi.



Obrázek 23: Zobrazení správného přiložení plochy prstu [11]

Otisk, který není uložený v databázi, je vždy správně posouzen jako neuložený. Tato výborná schopnost nepovolí neautorizovanému uživateli vstup do systému. Při testování, jsem ani jednou nenarazila na případ, kdy by senzor povolil přístup neautorizovanému uživateli. Tato schopnost by měla zajistit, že do systému nevnikne neoprávněný uživatel. Ovšem otisk, který je uložený, je rozpoznán v případě, že je poloha stejná jako při snímání. Je zde částečná variabilita pohybu, ale nepřesahuje více pár stupňů odklonění od středové osy oproti poloze při snímání. Otisk, který je posunut oproti původnímu snímání nahoru či dolů o několik milimetrů, není rozpoznán. Taktéž posunutí oproti původnímu snímání od svislé osy o zhruba 30° už není dostatečně spolehlivé.

V případě dodržení pravidel pro přiložení otisku prstu, je senzor poměrně spolehlivý. Uložené otisky jsou nalezeny. Vždy se zde najde nějaká chyba měření. Podrobné informace o těchto odchylkách naleznete v odstavci 5.3 Parametry vybraného senzoru otisku prstu. Statistika identifikace je níže v tabulce 9. Vzhledem ke neschopnosti senzoru rozpoznat otisk v jiné poloze musíme zvážit, jak vysoké zabezpečení požadujeme od systému. Tento senzor je dostačující k našemu použití. Bude aplikován jako přístup k napájecím automatům pro elektromobily nebo jako přístupový zámek do místnosti. Vzhledem k faktu, že zde není třeba zabezpečení na až tak vysoké úrovni, je tento senzor dostačující. V případě prolomení bezpečnosti v této problematice se jedná o malé ztráty. Potřebujeme-

li vyšší zabezpečení, je nutno zvážit výběr senzoru a úpravu systému. Mluvíme zde například o bezpečnosti osobních údajů, firemních tajemstvích či bezpečnosti různých, např. státních organizací. Spolehlivost senzoru je značně omezena na poloze při snímání otisku prstu. Tato chyba je pravděpodobně způsobena metodou rozpoznávání. V případě potřeby vyšší bezpečnosti biometrického systému je třeba zvážit senzor s jinou metodou rozpoznávání. Profesionální biometrické systémy s rozpoznáváním podle markantů, poznají shodu i při jiné poloze prstu, díky vzájemné poloze jednotlivých markantů. Senzor totiž vyhledá markanty, a vypočte jejich vzájemnou polohu, velikost či orientaci. 4.4.1Metoda založená na markantech

V případě testování uživatelů, kteří nejsou uloženi v databázi, se v mém měření nestalo ani jednou, že by se projevila shoda. Uživatel nebyl nikdy nalezen. Proces proběhl správně. Z toho faktu vyplývá, že míra chybného přijetí FAR je v mém případě FAR<0.001 %. Neuložený uživatel 10x testován, 10x nenalezen, je tedy 100% úspěšnost procesu.

V případě testování uživatelů, kteří jsou uloženi v databázi, se v mém měření stalo 4krát, že uživatel nebyl nalezen. Testování proběhlo 15krát, a pouze 11krát byl uložený uživatel skutečně nalezen. Proces proběhl správně. Toto testování je ovšem ovlivněno již výše zmíněnou polohou prstu na snímači. Proto nelze s jistotou říct, jaká je úspěšnost. Vše se odvíjí od polohy prstu na snímací ploše.

Číslo záznamu	Uživatel	Identifikační číslo uživatele	Vyhodnocení senzoru	Změna polohy prstu oproti snímání	Výsledek
1.	Uložen	19	Nalezen	Žádná nebo mírná	✓
2.	Uložen	21	Nenalezen	Posun horizontálně	—
3.	Uložen	24	Nalezen	Žádná nebo mírná	✓
4.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
5.	Uložen	28	Nalezen	Žádná nebo mírná	✓
6.	Uložen	31	Nalezen	Žádná nebo mírná	✓
7.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
8.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
9.	Uložen	36	Nenalezen	Posun vertikálně	—
10.	Uložen	44	Nalezen	Žádná nebo mírná	✓
11.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
12.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
13.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
14.	Uložen	27	Nenalezen	Posun horizontálně	—
15.	Uložen	53	Nalezen	Žádná nebo mírná	✓
16.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
17.	Uložen	57	Nalezen	Žádná nebo mírná	✓
18.	Uložen	64	Nalezen	Žádná nebo mírná	✓
19.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
20.	Uložen	4	Nalezen	Žádná nebo mírná	✓
21.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓
22.	Uložen	17	Nenalezen	Posun vertikálně	—
23.	Uložen	51	Nalezen	Žádná nebo mírná	✓
24.	Uložen	12	Nalezen	Žádná nebo mírná	✓
25.	Neuložen	Neexistuje	Nenalezen	Nemá vliv	✓

Tabulka 11: Přehled testování spolehlivosti senzoru

5.8.2. Přenositelnost dat mezi senzory

V rámci požadavku vytvořit plnohodnotný identifikační systém s více senzory, aby bylo možné jej umístit na více zařízení, bylo nutné vyzkoušet přenositelnost dat mezi senzory. Systém by měl obsahovat více senzorů, které budou fungovat v rámci jedné databáze. V databázi budou uloženi všichni uživatelé, kteří budou mít umožněn přístup. Proto byl zakoupen druhý senzor.

Byla vyzkoušena přenositelnost dat. Tento proces funguje za předpokladu, že senzor má stejné rozpoznávání otisků prstů. Je nutná shoda v komunikačním protokolu. Ovšem komunikační protokol se oproti rozpoznávání dá upravit, takže tento parametr není až tak podstatný. Vzhledem k faktu, že rozpoznávání probíhá uvnitř senzoru, a je naprogramované výrobcem, bylo třeba objednat druhý senzor, který je totožný. Předpokládáme ovšem, že rozpoznávání v senzoru probíhá na principu korelace. Protože doje k extrakci původních 9600 bytů na extrahovaných 196 bytů. Tyto byty jsou pak porovnávány v případě, že hledáme shodu. Tedy dva řetězce bytů, je byt po byte srovnáván. Tedy porovnávání dvou šablon otisku. 4.4.2 Metoda založená na korelaci. Dodavatel ovšem neposkytl podrobnější informace o jejich metodě.

Program obsahuje funkci, která otisk uloží do databáze. Další funkce, která uloží otisk zároveň do databáze i senzoru. V případě připojení dalšího senzoru k programu a databázi, lze stáhnout otisky v databázi uložené do dalšího senzoru. Ovšem všechno funguje za předpokladu, že senzor pracuje na stejném principu rozpoznávání a jeho zpracování otisku je stejné. Jinak by nebylo možné otisky podle uložených údajů identifikovat a verifikovat.

6. Závěr

Biometrie je věda, která využívá charakteristické měřitelné biologické struktury lidského těla k rozpoznávání osob. Fyziologické struktury jsou jedinečné a nezaměnitelné pro jedince. Díky této unikátnosti má jedinečné využití v oblasti identifikace osob. Práce se zabývá využitím otisků prstů pro identifikaci osob v oblasti elektromobility. Byl vytvořen systém pro identifikaci a verifikaci osob. Proběhl průzkum trhu týkající se biometrické techniky. Výběr čidla proběhl dle specifických parametrů. Pro identifikační systém Fingerprint recognition byl vybrán senzor firmy Waveshare. Vybraný senzor je poměrně spolehlivý. Potvrzení identity spočívá ve správné lokaci prstu uživatele.

Se senzorem otisku prstu byla zprostředkována komunikace a přenos dat. Byl vytvořen proces uložení uživatele, jeho identifikace a verifikace. Pro vytvoření programu byl využit programovací jazyk C# a vývojové prostředí Microsoft Visual Studio 2013. Aby byl systém plnohodnotný mohl být využit na více místech zároveň, byla vytvořena databáze. V databázi jsou uložená data uživatelů a je možno je přenést do dalších snímačů otisků prstů. Problematika databáze je řešena díky aplikaci phpMyAdmin. Správa databáze probíhá v prostředí HeidiSQL, která umožňuje práci s tabulkami a jejich obsahy.

Biometrické systémy se využívají v různých oblastech, například v odvětví průmyslu, pro různorodé bezpečnostní a přístupové systémy. Systém vytvořený v této práci může sloužit např. jako přístupový systém pro napájecí stanice pro elektromobily na VŠB-TUO či přístupový zámek na dveře při vstupu do místnosti. Implementace senzoru pro využití v napájecích automatech je obsahem jiné bakalářské práce.

Spolehlivost senzoru je poměrně značně omezena na poloze při snímání otisku prstu. Při změně polohy prstu je tato schopnost zcela omezena. Tato chyba je pravděpodobně způsobena metodou rozpoznávání. Protože senzor vytvoří šablonu otisku ve formě extrahovaných dat. Pak snímanou šablonu porovnává s referenčními šablonami uloženými v databázi. V případě potřeby vyšší bezpečnosti přístupového biometrického systému je třeba zvážit jinou metodu rozpoznávání. Profesionální biometrické systémy s rozpoznáváním podle markantů poznají shodu i při jiné poloze prstu, díky vzájemné poloze jednotlivých markantů.

V případě zdokonalení práce by se mělo jednat především o rozšíření celého systému. Doplnění dalších funkcí v programu, např. zobrazování otisků při identifikaci či verifikaci, automatická aktualizace dat při připojení senzoru. Dále doplnit databázi o možnost uložit ke každému uživateli více otisků prstů.

7. Seznam použité literatury

Knižní zdroje

[1] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

[2] RAK, Roman a Filip ORSÁG. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

[3] NÚDZIKOVÁ, Ing. Pavlína, Ing. Zdeněk SLANINA, PH.D., Ing. David VALA a Ing. Petr DRÁBEK. *Elektromobilita I: (Identifikace uživatele)*. Vysoká škola báňská – Technická univerzita Ostrava, FEI, 2014. ISBN 978-80-248-3531-0. Dostupné z:http://netfei.vsb.cz/downloads/autorske_texty/Elektromobilita%20I.pdf. Studijní materiály. VŠB – Technická univerzita Ostrava.

[4] JAIN, A.K., R. BOLLE a S. PANKANTI, eds. Biometrics: personal identification in networked society.Boston: Kluwer, c1999, x, 411 p. ISBN 978-0387-28539-9.

[5] DOBEŠ, Michal. *Rozpoznávání obrazu se zaměřením na identifikaci osob dle otisku prstu*. 1. vyd. Brno: VUT v Brně, 2000, 30 s. ISBN 80-214-1820-6.

[6] JAIN, Anil K. Introduction to biometrics. New York: Springer, c2011, xvi, 311 s. ISBN 978-0-387-77325-4.

[7] DRAHANSKÝ, Martin. *Biometric security systems fingerpring recognition technology: Biometrické bezpečnostní systémy technologie rozpoznávání otisků prstů : short version of Ph.D. thesis*. Brno: Vysoké učení technické, 2005, 32 s. ISBN 80-214-2969-0.

[8] FIŘT, Jaroslav a Radek HOLOTA. Digitalizace a zpracování obrazu.

[9] HSU, S.-H. a C.-L. HUANG. Road sign detection and recognition using matching pursuit method. *Image and Vision Computing*. 2001, vol. 19, issue 3, s. 119-129. DOI: 10.1016/S0262-8856(00)00050-0. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0262885600000500

[10] GREGORY, Peter H. a Michael A. SIMON. Biometrics for dummies. Hoboken : Wiley Publishíng Inc., 2008. xvi, 292 p. ISBN 978-0-470-29288-4.

[11] WAVESHARE ELECTRONICS. *UART Fingerprint Reader User Manual*. China, Shenzhen.

[12] ROBINSON, Simon. *C#: programujeme profesionálně*. Vyd. 1. Brno: Computer Press, 2003, xxx, 1130 s. Programmer to programmer. ISBN 8025100855.

[13] SHARP, John. *Microsoft Visual C# 2008: krok za krokem*. Vyd. 1. Brno: Computer Press, 2008, 592 s. ISBN 978-80-251-2027-9.

[14] SHARP, John. *Microsoft Visual C# 2010: krok za krokem*. Vyd. 1. Brno: Computer Press, 2010, 696 s. ISBN 978-80-251-3147-3.

[15] ŠONKA, Milan, Václav HLAVÁČ a Roger BOYLE. *Image processing analysis and machine vision*. 2nd ed. Pacific Grove: PWS Publishing, c1999, xxiv, 770 s. ISBN 053495393x.

[16] *Metody rozpoznávání a jejich aplikace*. Vyd. 1. Praha: Academia, 1993, 195 s. ISBN 80-200-0297-9.

Internetové zdroje

[17] Digitální obraz. MEFANET. *WikiSkripta: WikiSkripta, projekt sítě lékařských fakult MEFANET* [online]. 15.8.2010, 20.3.2014 [cit. 2014-11-26]. Dostupné z: http://www.wikiskripta.eu/index.php/Digit%C3%A1ln%C3%AD_obraz

[18] Biometriky nejen v pasech (1.). BITTO, Ondřej. *Lupa.cz: Server o českém internetu* [online]. 2005 [cit. 2015-01-18]. Dostupné z:http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/

[19] Krize daktyloskopie. KÁKONA, Martin. [online]. 2002 [cit. 2015-01-01]. Dostupné z: http://www.akademon.cz/source/biom.htm

[20] Technické hodnocení biometrických systémů. POLÁŠKOVÁ, Markéta. *Www.inovace.cz* [online]. Brno: JIC,Jihomoravské inovační cetrum, 11. červenec 2007 [cit. 2014-11-26]. Dostupné z: http://www.inovace.cz/novinky/727-technicke-hodnoceni-biometrickych-systemu

[21] Relační databáze. *Wikipedie: Otevřená encyklopedie.* [online]. 30. 10. 2014, 12:43 UTC [cit. 2015-04-01].Dostupné z:http://cs.wikipedia.org/w/index.php?title=Rela%C4%8Dn%C3%AD_datab%C3%A1ze&oldid=11965225

[22] MARC DELISLE. *PhpMyAdmin* [online]. [cit. 2015-03-19]. Dostupné z: http://www.phpmyadmin.net/home_page/index.php

[23] MySQL (23) - relace 1:N a N:N. PROVOZOVATEL: PAVEL KYSILKA, IČ: 72868490 (2003-2015). *Linuxsoft.cz* [online]. 3.6.2005 07:00 [cit. 2015-03-21]. Dostupné z: http://www.linuxsoft.cz/article.php?id_article=854

[24] RS-232. *Wikipedie: Otevřená encyklopedie.* [online]. 9. 9. 2014, 16:53 [cit. 2014-12-01]. Dostupné z:http://cs.wikipedia.org/wiki/RS-232

8. Seznam příloh

I. Návod Fingerprints- *Návod k programu Fingerprints*
II. Návod Fingerprint lock- *Návod k programu Fingerprint lock*
III. Fingerprints *(Příloha na DVD)-zdrojový kód programu*
IV. Fingerprint lock *(Příloha na DVD)- zdrojový kód programu*
V. Waveshare datasheet *(Příloha na DVD)- manual k senzoru otisku prstu*

I. Návod Fingerprints

Děkuji, že jste si vybrali biometrický program Fingeprints Recognition pro rozpoznávání otisků uživatelů.

Připojte senzor otisku prstu. Při prvním použití senzoru musíte nainstalovat CP210x USB to UART Bridge VCP Drivers. V případě, že tento program nenainstalujete, senzor nebude komunikovat.

Tento program slouží pro vykreslení otisku prstu, ukládání uživatelů do databáze senzoru. Mezi další funkce patří identifikace uživatele, verifikace uživatele, smazání vybraného uživatele, či celé databáze uživatelů, extrakce dat reprezentující otisk prstu pro jeho následovné uložení. Dále zde naleznete uložení uživatele také do databáze phpMyAdmin. Opětovné načítání údajů uživatelů z databáze phpMyAdmin. Načtené údaje jde lze opětovně uložit do senzoru.

Spusťte instalační balíček a nainstalujte program. Před spuštěním programu připojte senzor. Poté můžete program spustit.

Vykreslit otisk: Pro vykreslení otisku prstu přiložte prst ke snímací ploše senzoru a klikněte na tlačítko „Sejmi otisk“. Otisk se vykreslí na dvou obrázcích, v menší a větší variantě.

Uložení uživatele do databáze senzoru: pro uložení vyplňte pole „Vlož ID uživatele“ a pole „Oprávnění uživatele“. ID (identifikační číslo) uživatele je kladné celé číslo. Oprávnění uživatele má tři úrovně: 1,2,3. Tímto omezíte přístup uživatele k určitým oblastem. Po vyplnění údajů kliknout na tlačítko „Přidej uživatele“.

Verifikace uživatele: Verifikace probíhá na základě Vámi známém ID uživatele. Verifikace je potvrzení totožnosti požadovaného uživatele. Napište tedy do pole „Vlož ID uživatele“ identifikační číslo uživatele, kterého znáte. ID(identifikační číslo) uživatele je kladné celé číslo. Klikněte na tlačítko „Verifikuj“ pro provedení úkonu. Program vrátí hlášku, zda byl proces úspěšný.

Identifikace uživatele: slouží k nalezení majitele otisku prstu v databázi. Přiložte tedy prst ke snímací ploše senzoru, a kliknout na tlačítko“Identifikuj“. Systém vypíše, zda nalezl či nenalezl shodu.

Vymazat uživatele: vymazat můžete jednoho uživatele nebo celou databázi senzoru. V případě vymazání celé databáze jen kliknout na tlačítko “Vymazat všechny uživatele“. V případě vymazání konkrétního uživatele vyplňte pole „Vlož ID uživatele“ a klikněte na tlačítko “Smaž vybraného uživatele“. ID (identifikační číslo) uživatele je kladné celé číslo. Program vrátí hlášku, zda byl proces úspěšný.

Databáze:

Databáze je vytvořena na serveru rc111- CPIT, (Vědecko-výzkumné laboratoře Vysoké školy báňské). Databáze vytvořena v programu phpMyAdmin nese název jan0389. Na server se dostanete odkazem: http://rc111.vsb.cz/phpmyadmin/index.php?token=c223928a4cc4b33d7136dd7841c85996&old_usr=jan0389.

Pro přihlášení potřebujete Jméno a Heslo. *(na vyžádání)* V této databázi jsem vytvořila dvě tabulky. Tabulka *fingerprint* nese údaje o uživateli a data pro otisk prstu. Tabulka *pristupovadata* poskytuje údaje o zápisu uživatele do databáze.

fingerprint				
Pole	**Typ**	**Nulový**	**Výchozí**	**Další**
id	int(11)	Ne	žádná	AUTO_INCREMENT
jmeno	varchar(80)	Ne	žádná	
fingerprintdata	varchar(630)	Ne	žádná	
privilegelevel	int(11)	Ne	žádná	
stav	varchar(20)		žádná	
pristupovadata				
Pole	**Typ**	**Nulový**	**Výchozí**	**Další**
id	int(11)	Ne	žádná	AUTO_INCREMENT
id_fingerprint	int(11)	Ano	Null	
datetime	timestamp	Ne	CURRENT_TIMESTAMP	

Tabulka 1: Struktura polí tabulek databáze

Vypsané parametry, tedy strukturu tabulky, lze dle potřeb změnit. Upravit můžete u vybrané tabulky v záložce Struktura. Pro správu databáze můžete využít HeidiSQL. Umožňuje práci s tabulkami a jejich obsahy. Například prohlížení a úprava dat, vytváření a úprava tabulek, apod. V HeidiSQL se nastavují cizí klíče v databázi. Po stažení a nainstalování HeidiSQL se přihlásíte do databáze jan0389 pomocí IP adresy serveru a přiděleného jména a hesla. V případě zájmu lze vytvořit vlastní databázi.

Komunikace s databází:

Uložení do DB jan0389 a do DB senzoru: Pro uložení uživatele do databáze jan0389 a zároveň do databáze senzoru vyplňte horní pole „Jméno uživatele“ a „Oprávnění uživatele“. Pro provedení uložení kliknout na tlačítko „Ulož do DB a senzoru“. Program vrátí hlášku, zda byl proces úspěšný.

Uložení do DB jan0389: Další funkce je uložení dat pouze do databáze jan0389. Pro uložení uživatele do databáze jan0389 vyplňte horní pole „Jméno uživatele“ a „Oprávnění uživatele“. Pro provedení uložení kliknout na tlačítko „Ulož do DB“. Program vrátí hlášku, zda byl proces úspěšný.

Načíst data z DB: Funkce pro načtení dat z databáze kliknout na tlačítko „Načti z DB“. Program vrátí údaje do polí „Jméno uživatele“, „Oprávnění uživatele“, „ID uživatele“ a „Data“. Pole data obsahuje extrahovaná surová data charakterizující otisk prstu.

Uložení do DB senzoru: Další funkce je uložení dat pouze do databáze senzoru. V případě, že jste načetli data z databáze, nevyplňujte žádné pole. Jen kliknout na tlačítko „Uložit data do senzoru“. V opačném případě uložení uživatele do databáze senzoru vyplňte dolní pole „Jméno uživatele“, „Oprávnění uživatele“, „ID uživatele“, „Data“. Pro provedení uložení kliknout na tlačítko „Ulož do DB“. Program vrátí hlášku, zda byl proces úspěšný.

Do pole „data“ vkládáme surová data. Tedy data extrahovaná pro daný otisk prstu, ale zbavená hlavičkových dat (byty), startovního a koncového bytu, hodnoty checksum. Jedná se o 196 bytů.

II. Návod Fingerprint lock

Děkuji, že jste si vybrali biometrický program Fingerprint lock pro rozpoznávání otisků uživatelů.

Připojte senzor otisku prstu. Při prvním použití senzoru musíte nainstalovat CP210x USB to UART Bridge VCP Drivers. V případě, že tento program nenainstalujete, senzor nebude komunikovat.

Popis programu: Fingerprint lock je program sloužící k přístupu do systému. Využívá pouze identifikaci uživatele. Do databáze uložte jen otisky uživatelů, kterým chcete povolit přístup. Po potvrzení identifikace je povolen přístup danému uživateli. V opačném případě program nabídne opětovnou identifikaci. Podrobnější rozdělení přístupu uživatelů se dá specifikovat pomocí nastavení úrovně oprávnění přístupu. Identifikace probíhá neustále dokola v cyklu. Systém je propojen s databází. Tento program je možno využít jako zámek oprávněného vstupu do místnosti. V programu se při potvrzení identifikace vyvolá metoda povolení přístupu (např. otevření dveří.). Do této metody uložte kód pro otevření dveří.

Identifikace uživatele: Při spuštění programu automatické spuštění identifikace (senzor modře svítí). Systém vypíše, zda nalezl či nenalezl shodu. V obou případech nabídne novou identifikaci.

Databáze:

Databáze je vytvořena na serveru rc111- CPIT, (Vědecko-výzkumné laboratoře Vysoké školy báňské). Databáze vytvořena v programu phpMyAdmin nese název jan0389. Na server se dostanete odkazem: http://rc111.vsb.cz/phpmyadmin/index.php?token=c223928a4cc4b33d7136dd7841c85996&old_usr=jan0389.

Pro přihlášení potřebujete Jméno a Heslo. *(na vyžádání)* V této databázi jsem vytvořila dvě tabulky. Tabulka *fingerprint* nese údaje o uživateli a data pro otisk prstu. Tabulka *pristupovadata* poskytuje údaje o zápisu uživatele do databáze. Připojení slouží v získání jmen uživatelů.

fingerprint				
Pole	**Typ**	**Nulový**	**Výchozí**	**Další**
id	int(11)	Ne	žádná	AUTO_INCREMENT
jmeno	varchar(80)	Ne	žádná	
fingerprintdata	varchar(630)	Ne	žádná	
privilegelevel	int(11)	Ne	žádná	
stav	varchar(20)		žádná	
pristupovadata				
Pole	**Typ**	**Nulový**	**Výchozí**	**Další**
id	int(11)	Ne	žádná	AUTO_INCREMENT
id_fingerprint	int(11)	Ano	Null	
datetime	timestamp	Ne	CURRENT_TIMESTAMP	

Tabulka 1: Struktura polí tabulek databáze

Vypsané parametry, tedy strukturu tabulky, lze dle potřeb změnit. Upravit můžete u vybrané tabulky v záložce Struktura. Pro správu databáze můžete využít HeidiSQL. Umožňuje práci s tabulkami a jejich obsahy. Například prohlížení a úprava dat, vytváření a úprava tabulek, apod.

V HeidiSQL se nastavují cizí klíče v databázi. Po stažení a nainstalování HeidiSQL se přihlásíte do databáze jan0389 pomocí IP adresy serveru a přiděleného jména a hesla. V případě zájmu lze vytvořit vlastní databázi.